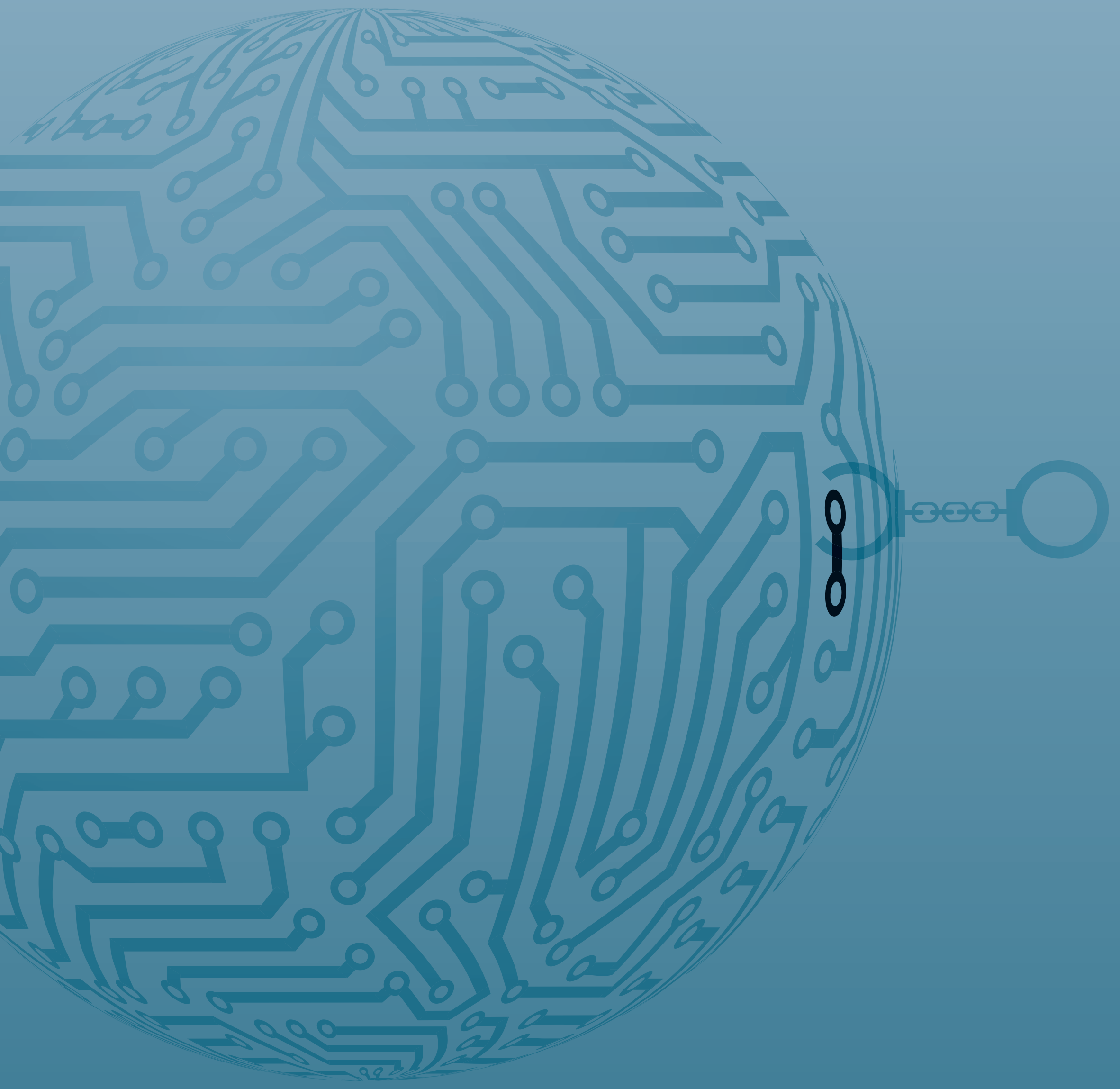
Cybercrime Investigation Body Of Knowledge

2nd Edition

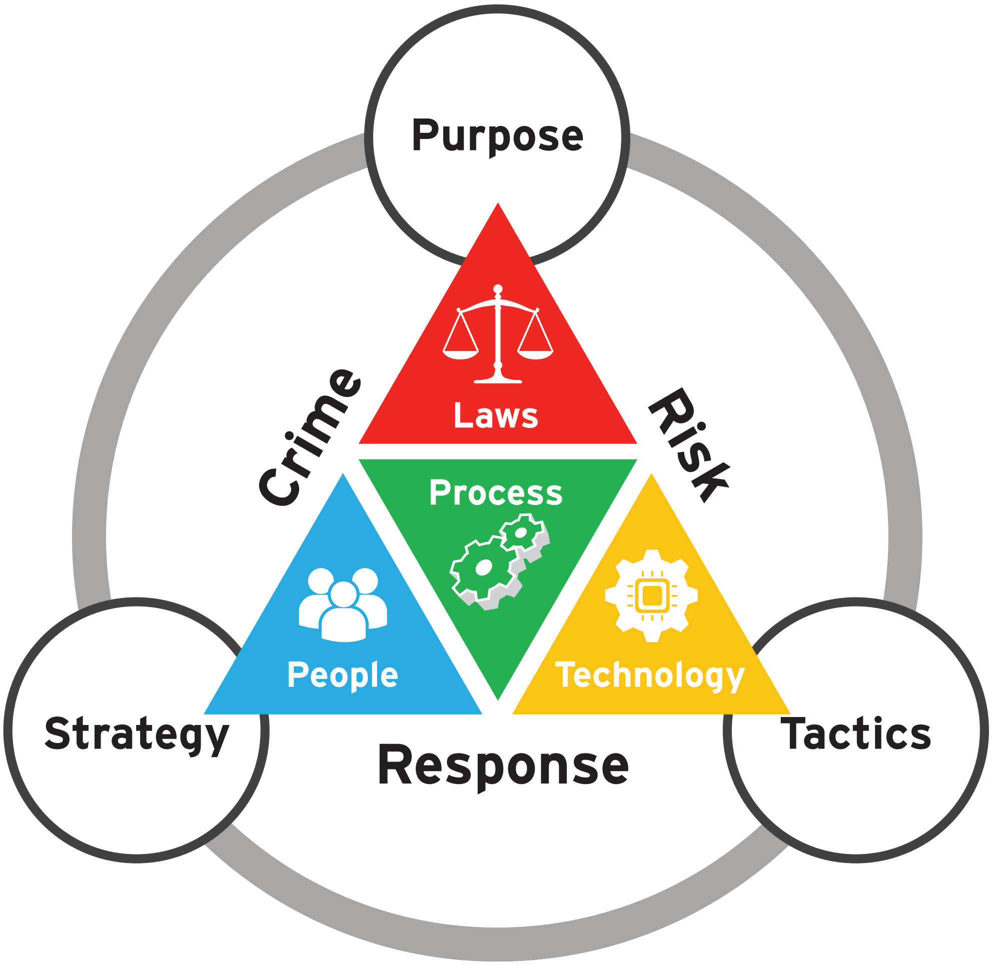
Cybercrime Investigation Body Of Knowledge
2nd Edition



A Guide to the

Cybercrime Investigation Body of Knowledge

(CIBOK Guide 2nd Edition)



Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

First edition　Jan.2017
Second edition　May 2025

On the Occasion of the Publication of CBOK Ver. 2

Cybercrime is becoming an increasingly serious issue in modern society. As technology evolves, cybercriminals are enhancing their methods, causing significant impacts on our lives and social infrastructure. The financial damages are increasing yearly, affecting businesses, government agencies, and individuals. In response to this reality, CIBOK (Cybersecurity Incident Management Body of Knowledge) has been updated to Ver. 2.0 to provide a practical framework for addressing the threats posed by cybercrime.

Several key reasons underpin this revision. First, the growing severity of cybercrime's impact on society is undeniable. Cybercriminal tactics have diversified, and their scope has broadened. In addition to traditional methods such as corporate data theft and ransomware attacks, new threats, including state-level cyberattacks and AI-driven techniques, have emerged. In this environment, sharing up-to-date information and swiftly implementing effective countermeasures is essential.

Second, while the number of cybersecurity professionals is increasing, there remains a shortage of experts with specialized knowledge and experience in combating cybercrime. Many technicians are tasked with security measures, but their threats extend beyond technical issues to legal, social, and ethical challenges. To address these complexities, CIBOK Ver. 2.0 has been revised to provide relevant content for a wide audience, aiming to benefit experts and a broad range of individuals.

Third, cybercrime's effects are not limited to law enforcement agencies and professionals; they impact everyone. Even those not directly involved in cybersecurity can be affected. In today's interconnected world, everyone must have a basic understanding of cybercrime. Therefore, this publication comprehensively covers topics from foundational concepts of cybercrime to specific measures organizations and individuals can take. It provides accessible and beneficial content for general readers, law enforcement, and security professionals.

Moreover, CIBOK Ver. 2.0 offers over 500 pages of enhanced countermeasures, encompassing extensive knowledge required for modern cybercrime response. To ensure broader accessibility, the book is being published simultaneously in English and Japanese, facilitating information sharing with a global audience and promoting international cybersecurity efforts.

Maintaining sustainable business growth while aligning with organizational balance and strategy is also increasingly important when considering countermeasures. CIBOK Ver. 2.0 emphasizes the following key aspects:

- Comprehensive explanation of the latest cybercrime trends: Detailed analysis of emerging threats and evolving criminal techniques.
- Enhanced practical incident management processes: Specific countermeasures and actionable guidelines for real-world application.
- Improved accessibility for a wider audience: Incorporating explanations of technical terms and crime prevention tips applicable to daily life to expand the readership.
- This book aims to serve as a guide for accurately understanding and appropriately responding to cybercrime threats. We hope each reader deepens their knowledge of cybersecurity and contributes to realizing a safer society.

Hiroshi Nishino
Chairperson of the CIBOK Editorial Committee

Foreword

When asked by one of the authors to write the forward for this invaluable, comprehensive, and detailed book on cybersecurity investigations, of course I said yes. I have worked with the authors and experienced their dedication and passion. All are experts in their respective fields and have unparalleled real-life working knowledge and experience, having spent most of their careers fighting cybercrime globally. They are global warriors, "the best of the best," sharing their knowledge collectively to compile this incredible resource.

My initial thought was what an honor it was to be asked. Secondly, I wondered how I could get you- the reader- to realize the significance of the insights and knowledge shared in this book so that it becomes a must-read. Whether you are a seasoned professional or just starting your career in cybersecurity investigations, this book has something for everyone including you. It will increase and augment your working knowledge in this field.

You are about to embark on what I find to be a remarkably interesting and rewarding journey to increase your cybercrime investigations knowledge. The gap is widening between cybercriminals, nation-state actors, bad actors, and miscreants, and people like you who are focused on fighting cybercrime and disrupting organized crime groups. These cyber criminals and groups operate with impunity most of the time and have little fear of being caught. Their methods and tactics are highly sophisticated and extremely lucrative. It is not easy to identify who is behind cyber crimes, identify their network infrastructures, and disrupt them. Cybercrimes are insidious and, most of the time, borderless.

Sharing information collectively, cooperatively, and globally across industries and law enforcement and turning that information into intelligence is paramount. It can take years to gather all of the intelligence required to develop a case. It requires global cooperation and coordination with trusted entities, industries, and federal law enforcement agencies to build a case and prosecute.

A particularly good example of this is the takedown of GameOver ZeuS (GOZ) in 2014. GOZ was an extremely sophisticated malware designed to steal bank information and credentials from infected computers. It was responsible for damages of over $100 million in bank fraud and was the main vehicle used for the CryptoLocker ransomware attack. It took over two years to gather all of the necessary intelligence, map out the technical infrastructure, collect evidence to build the case for the takedown of the botnet, and get indictments in place. This required a strategic operational plan, multinational coordination, and cooperation.

The takedown was led by the Federal Bureau of Investigation (FBI). They worked with private industry and highly technical companies in the US, across US federal agencies, and with over 10 law enforcement agencies worldwide in a coordinated, collective, and cooperative effort to take down and disrupt this sophisticated botnet.

In 2014, a federal grand jury in Pittsburgh, PA unsealed a 14-count indictment against Evgeniy Mikhailovich Bogachev of Anapa, Russian Federation for his alleged role as an Administrator of the GameOver ZeuS botnet. He was placed on the FBI' s Cyber Most Wanted list and a $3 million bounty was offered for information leading to his arrest or conviction. This amount was unheard of at the time.

Today, Evgeniy Mikhailovich Bogachev remains a free man working and living in Russia using his real name. He is protected.

It is extremely difficult and time-consuming to gather all of the necessary evidence and prosecute a cybercrime, and in some cases criminals are already protected in certain countries and operate with impunity. It is imperative that investigators avoid making mistakes that add to the challenge during the investigative process. The Cybercrime Investigation Body of Knowledge will increase your chances of success in the investigative process.

Since the first edition of Cybercrime Investigation Body of Knowledge in 2017, there have been numerous technological advances that have enabled the acceleration of cybercrime and criminals' capabilities, techniques, and methods- Artificial Intelligence (AI) being one of them. It is more imperative than ever to take a proactive, preventative approach to cybersecurity, cyber investigations, and overall security. Constant vigilance and due diligence are critical in all areas of cybersecurity. Cybercrime is not a victimless crime. All of us play a role in fighting cybercrime and maintaining overall security. This endeavor is not for the curious- it is for the committed. It is only through our global collective, cooperative efforts increasing our cybercrime knowledge and expertise and sharing information that we can create a safe cyber future.

I am certain this book will prove to be an invaluable resource to anyone compelled to increase their knowledge regarding cybersecurity investigations. Enjoy the read and may your excellent work contribute to numerous cybercrime prosecutions.

Maria J. Vello
May 20, 2024

Maria Vello is a cybercrime veteran with decades of experience bridging the gap between public and private sectors to advance threat intelligence and cybercrime investigations. Maria is the former President and CEO of National Cyber Forensics Training Alliance (NCFTA) in the USA and the former CEO of Cyber Defense Alliance (CDA) in the UK.

Authors

Executive Editor

Shane Shook (PhD) is a well-known veteran of information security and response engagements with nearly 30 years of experience spanning government and industry IT risk management issues. He has led forensic analysts and provided expert testimony in many of the most notorious breaches across most industry sectors. He has also served as expert witness in related (international and US) federal, civil and commercial disputes. He currently serves on the advisory boards of several emerging security technology companies. He is a contributing author and editor of several books and a frequent keynote or guest speaker.

Authors and contributors to this edition of CIBOK

Aaron Goldstein is a cyber incident response leader and researcher. He has experieince in complex, large-scale cyber breaches where he has provided strategic solutions to secure environments of all sizes.

Alberto Casares is a threat intelligence researcher and analyst, and CTO of Constella Intelligence where he focuses on identity threat detection and response. He has led several research & development projects supported by the Spanish Ministry of Industry and is a Cybersecurity professor for the University of Granada Master's in Cybersecurity degree program.

Antonia Nisiota (PhD) is a cyber Security Operations Center leader, researcher and analyst with specialties in security posture management, threat hunting, and computer and memory forensics.

Billy Gouveia is the CEO and Founder of SureFire, Inc. He has more than 20 years' experience spanning cyber incident response, intelligence collection and analysis, and technology.

Bradley Potteiger (PhD) is Co-Founder and Chief Technology Officer of ArmsCyber. He has intelligence collection, cyber defense, analysis, and technology development experience from government and industry organizations, including the US Department of Defense. He has developed specialized experience in active defense methods utiilzing zero trust, automated moving target defense, deception technologies, and recovery principles of cyber security. He has taught and performed academic research at the University of Maryland and The Johns Hopkins University Applied Physics Laboratory on topics of cyber security, autonomous vehicle security and privacy, election integrity, space systems, and national security.

Chris Coulter is a forensic examiner and incident responder who has led engagements in government, industry, and individual computer crimes investigations. He is a patent holder (Digital forensic acquisition kit and methods of use thereof - United States US 13/019,796) for technology that he developed and delivered to the market to simplify the complex methods of evidence acquisition in forensic computer investigations. His experience includes corporate leadership in cyber security services and products, audit and investigations experience with PwC, Stroz Friedberg LLC, MIT

Labs, and the IRS.

Dan Gunter is the founder and CEO of Insane Cyber, a cyber threat hunting and forensics firm focused on IT and OT networks. He has extensive OT and industrial control systems cyber security research and incident response experience gained from working with clients in Oil and Gas, and global Energy companies. He also served as a USAF Cyber Warfare Officer in the AFCERT and CYBERCOM teams.

David Emerson has extensive leadership experience from Chief Information Security and Technology roles with several product and services companies. He is CTO of SolCyber, a Managed Security Services Provider who help to ensure secure program and operational posture for their clients.

Erin Joe is a Senior Executive at Mandiant in Google's Office of the CISO. After a 25 year career culminating as a Senior Executive in the FBI, she joined Mandiant and Google to apply her experience in cyber crime investigation and crisis response.

Hideki Ninomiya is CEO and Founder of Orient Co., Ltd. He has an extensive career of both IT leadership and cyber security and cyber crime analysis and risk advisory services spanning Pharmaceuticals and other industries in Japan. He also advises boards of companies about cyber risks and security organization and posture development.

Hiroshi Nishino is a Chairperson of the CIBOK Editorial Committee, CEO of HI Initiative Co., Ltd. In 1991, he founded Proseed Co., Ltd. and introduced numerous global standard knowledge systems such as PMBOK, ITIL, and COPC into Japan. He contributed to the establishment of promotion organizations for PM, ITSM, and CIKF. Additionally, since 2001, he has been involved in government IT procurement reform, participating in various government committees to propose and implement comprehensive bidding systems, CIO advisor systems, and human resource development initiatives. Concurrent Roles : Vice Chairman of the Board, CeFIL (Specific Nonprofit Corporation); Co-founder of the Digital Business Innovation Center; Member of the Global Cybercrime Experts Committee, International Criminal Police Organization (Interpol); Co-founder and Board Member of the Cybercrime Investigation and Research Forum, a general incorporated association; Part-time Lecturer at the Graduate School of Information and Life Sciences, University of Tsukuba; Part-time Lecturer, Liberal Arts Education, University of Toyama.

Ian (Iftach) Amit is a seasoned manager in the security and software industry with vast experience in a myriad areas of information security- from enterprise security, through retail, to end user software and large back-end systems. He is an Information Security expert with experience ranging from low level technical expertise and up to corporate security policy, regulatory compliance and strategy. Ian is a frequent BlackHat and DefCon speaker, and founding member of the PTES (Penetration Testing Execution Standard), IL-CERT, and the Tel-Aviv DEFCON group (DC9723).

Karim Hijazi is an investor and cyber security intelligence leader with over 30 years of practical experience in cyber security and intelligence. He founded several cyber intelligence services companies to address global botnets and their impact on government organizations and private companies.

Kathryn Shih is a cyber security analyst, investor, and practitioner with cloud and artificial intelligence program development and management specialties gained in organizations including Akamai Technologies, Amazon Web Services, and Google.

Kelly Robertson has more than 30 years of professional cyber security experience spanning 30 countries. He has held key technical and market positions with leading ICT and cyber security companies including SAIC, Nokia, Juniper Networks, White Hat Security, Atos, and Horizon3.ai. His contributions from hands-on technical program development, training, and market defining activities has been helpful in the perspectives provided in this edition. He is a long time friend and colleague of Dr. Shook, with whom he has collaborated for more than 20 years on advancing themes of recognizing and addressing cyber risks through effective programs and processes.

Maria Vello is a cybercrime veteran with decades of experience bridging the gap between public and private sectors to advance threat intelligence and cybercrime investigations. Maria is the former President and CEO of National Cyber Forensics Training Alliance (NCFTA) in the USA and the former CEO of Cyber Defense Alliance (CDA) in the UK.

Mark Mullison is the Chief Technology Officer of Allied Universal, and has more than 30 years of technology and cyber security leadership experience spanning telecommunications, education, and physical security industries.

Neil Binnie (PhD) is a senior cyber security Executive with experience spanning Global Construction and Real Estate, and Aerospace.

Noriaki Hayashi is a Senior Researcher with Trend Micro Incorporated in Japan. He is a highly-skilled and certified administrator and systems engineer in several computing platforms and technologies. He has more than 17 years of systems management and security experience, including program and project management, security research, and threat response.

Omalola Fagbule (PhD) is a Cyber security Awareness Specialist and researcher focused on understanding human motivation and perceptions. She develops training programs and materials addressing the motivations and actions of cyber criminals to educate staff and raise organizational awareness.

Patrick A. Westerhaus joined Wells Fargo in 2016 and is heading up a team in Enterprise Information Security (EIS), Cyber Threat Fusion Center (CTFC), working to consolidate and analyze data in an effort to develop an enterprise program to reduce cyber, fraud, and money laundering risk for the institution. Prior to joining Wells Fargo, Patrick was with KPMG in their fraud and forensic practice and he spent the last 12 years in the FBI reaching the level of Supervisory Special Agent in the Headquarters Cyber Division. During his tenure in the FBI Patrick led investigations into corporate/

government fraud, public corruption, counterterrorism, counterintelligence, cyber fraud/theft and his last position was at the NCIJTF' s Virtual Currency Team. Patrick has a Bachelor of Business Administration in accounting from Gonzaga University, a Masters in Forensic Science in Security Management from The George Washington University, and a graduate certificate in International Security from Stanford. Patrick also is a CPA and he maintains CFE & CAMS certifications.

Satoshi Shimizu is a founder of the Cybercrime Investigations Knowledge Forum and editor of the first edition of the Cybercrime Investigation Body of Knowledge. He has an extensive career leading technology and cyber security products and programs development for Trend Micro as a Regional CISO for the Japan BU, and as a Director of the Japan Cybercrime Control Center, and of an INTERPOL alliance project with Trend Micro - he has helped to define international intelligence and response efforts to global combat cybercrime.

Scott McCready is CEO of SolCyber and has led cyber security products and services delivery around the world for some of the best-known security companies including FireEye, Symantec, NTT, and EDS.

Simon Mullis is an experienced cyber security products and services executive who has led teams at FireEye, Palo Alto Networks, Tanium, and cofounded Venari Security as Chief Technology Officer. He also has represented industry and public sector needs of cyber security as a public speaker at technology and security conferences across Europe and North America.

Tammy Archer has extensive cybersecurity leadership experience as the CISO of Inchcape PLC, a global automotive distribution services company, and former CISO of HSBC. She previously served the UK Government as CISO of the Foreign and Commonwealth Office, and in the UK Ministry of Defence, and the Royal Navy.

Wajih Yassine is a senior cyber security and forensics engineer with experience gained supporting Google and Cylance customers. He has contributed to the development of cloud and enterprise forensics tools.

Special thanks to the contributions to this edition from the following companies:

Orient Co. Ltd - Japan
Trend Micro - Japan
Acora - UK
Surefire Cyber - USA
SolCyber - USA
Insane Forensics - USA
Forgepoint Capital - USA

And continuing thanks to the following contributors to the first edition of CIBOK

Craig W. Sorum is a veteran of the Federal Bureau of Investigation (FBI) where he conducted and supervised hundreds of domestic and international cybercrime investigations while assigned to field offices in El Paso, TX, Washington, D.C., Cedar Rapids, IA and Minneapolis, MN. Craig received awards for significant cyber investigations as a field agent and was selected as a "Federal 100 Award" winner for top IT managers in government for his accomplishments as Chief of the FBI's Law Enforcement Online Unit at FBIHQ. Following the Bureau, Craig was employed as a Senior Manager of Information Security at a Fortune 500 defense and aerospace company where he was responsible for all cyber investigations and threat intelligence matters. Craig is currently working as a cyber security management consultant.

David Cowen is a Certified SANS Instructor, CISSP, and GIAC Certified Forensic Examiner. He has been working in digital forensics and incident response since 1999 and has performed investigations covering thousands of systems in the public and private sector. Those investigations have involved everything from revealing insider threats to serving as an expert witness in civil litigation and providing the evidence to put cyber criminals behind bars. David has authored three series of books on digital forensics; Hacking Exposed Computer Forensics (1st-3rd editions), Infosec Pro Guide to Computer Forensics, and the Anti Hacker Toolkit (Third Edition).

Eric Zimmerman is a Senior Vice President in Kroll's Cyber Security and Investigations practice. Eric has a tremendous depth and breadth of expertise in the cyber realm, spanning complex law enforcement investigations, computer forensics, expert witness testimony, computer systems design and application architecture. He has received numerous recognitions for his work, is an award-winning author and is a frequently sought-after instructor and presenter on cyber-related topics. Before joining Kroll, Eric was a Special Agent with the Federal Bureau of Investigation (FBI), specializing in investigating criminal and national security-related computer intrusions, crimes against children (production, distribution and possession of child pornography), intellectual property theft and related crimes.

John Jolly is a seasoned cybersecurity executive with a breadth of industries experience. John served as the Vice President and General Manager of the Cyber Security Division at General Dynamics, where he had responsibility for a broad portfolio of products and services that included a commercial incident response practice. John holds an undergraduate degree in Computer Science with honors from the University of Maryland Baltimore County and a MBA in Finance with honors from the Wharton School at the University of Pennsylvania.

Judith H. Germano is the founding member of GermanoLawLLC, a law firm specializing in advising companies on cybersecurity governance and data privacy issues. Ms. Germano is an Adjunct Professor at New York University School of Law and a Senior Fellow at the New York University (NYU) Center for Cybersecurity, where she leads NYU' s task force of corporate executives and senior government officials focusing on emerging cybersecurity issues and solutions. Previously, Ms. Germano served as Chief of Economic Crimes at the U.S. Attorney' s Office for the District of

New Jersey, and was a federal prosecutor for 11 years. Before joining the U.S. Attorney's Office, she worked at the multinational law firm Shearman & Sterling LLP, in New York City. Ms. Germano' s publications include Cybersecurity Partnerships: A New Era of Collaboration, and After the Breach: Cybersecurity Liability Risk.

Luke Dembosky is a Partner in Debevoise & Plimpton's Cybersecurity & Data Privacy group and formerly served as Deputy Assistant Attorney General for National Security at the Justice Department's National Security Division. Over 14 years with DOJ, he has served in various roles, including as Deputy Chief for Litigation at DOJ's Computer Crime and Intellectual Property Section. Mr. Dembosky has been a regular advisor to the leadership of the DOJ, FBI, Secret Service, National Security Council and other agencies regarding major cyber cases and related legal and policy issues. He participated in the negotiation of a 2013 cyber accord with Russia and the historic 5-point agreement signed by President Obama and President Xi Jinping of China in 2015, and has co-represented DOJ in cyber discussions at the United Nations. He was recently named Vice Chair of the ABA Public Contract Law Section, focusing on addressing technology risks to supply chain. Mr. Dembosky is also Co-Chair of the Information Sharing and Analysis Organization Governance Working Group leading the development of internal governance guidance for ISAOs as part of the White House initiative to establish cybersecurity threat sharing platforms across industry.

Philip Fodchuk leads Suncor's Enterprise wide Information Security Program. Within Suncor, Philip is responsible for maturing and enhancing the information security posture of the organization, and leads the cyber security incident response function. Previously, Philip was a Partner with Deloitte's Cyber Security practice within the Enterprise Risk Services group. In that role he served as a Global leader for Crisis Management for the Energy & Resources sector and was Deloitte' s Canadian leader for Cyber Security Incident Response. Philip was a sworn police officer with the Royal Canadian Mounted Police (RCMP) and the Calgary Police Service where he worked with technological crime, cyber security and incident response matters. With 20 years of diverse experience, Philip is considered a subject matter expert in responding to, managing and developing strategies around cyber security, digital forensic, incident management and organizational crisis issues.

CIBOK Table of Contents

CIBOK Table of Contents 13

Chapter 1: Cybercrime and its Investigation 51

Chapter 2: Types of Cybercrimes 75

Chapter 3: Artifacts of Cybercrime 105

Chapter 4: Scope of Cybercrime 135

Chapter 5: Sources of Evidence 169

Chapter 6: Methods of Evidence Collection 213

Chapter 8: Resolution 303

Chapter 11: Practical Cyber Risk Management 403

Appendices 431

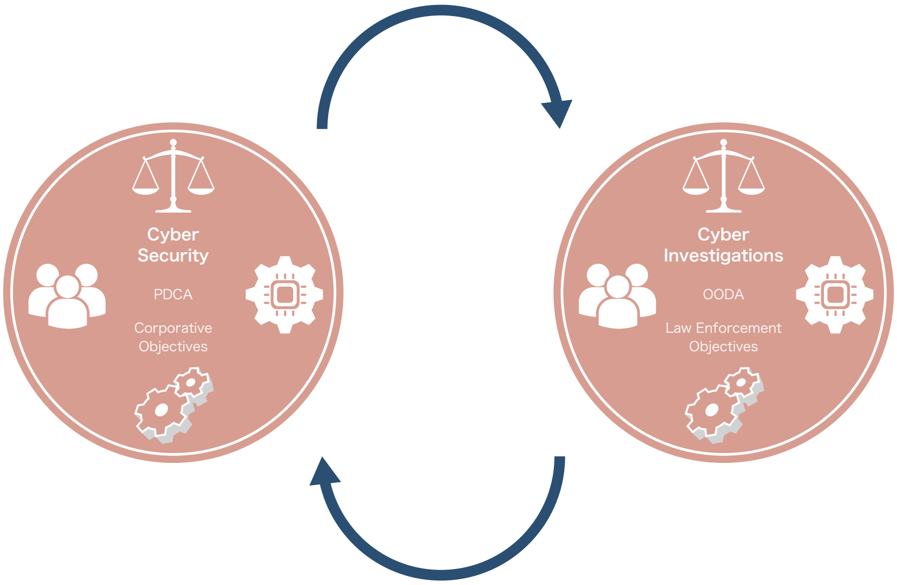
Introduction

Introduction to the Guide

Target Readers

The following groups and individuals are the target readers for this document.

- Police organizations or law enforcement agencies (prosecutors, courts, etc.) conducting criminal investigations, staff members of organizations conducting similar professional duties (such as organizations with recognized police powers including the right to investigate, the right to arrest, etc.), staff members investigating organizational misdeeds, and persons with criminal investigation experience who are unfamiliar with "cybercrime"
- Persons in charge of forming and commissioning new in-house cybercrime investigation teams
- Executive trainees who have prior experience managing actual in-house criminal investigations, and who expect to be appointed to cybercrime investigation divisions in the future
- Persons who conduct research/development/instruction in programs which train cybercrime investigators and exhibit a high level of effectiveness in a short period of time



Same coin, different focus

Green Eggs and SPAM- Efficient Incident Response

There once was some data on a computer
Created by a user that nobody knew
It was taken by someone who didn't exist
And that's when the incident grew

Two other computers had malware
Another had anomalous comms
To blacklisted IP addresses
So everyone worried about (logic) bombs

...and droppers, downloaders and Trojans
Anonymous, the Chinese, and Shamoon…

But no one stepped back for a second
to try to think the whole thing through.

Turned out that the computer was accessed
by Bob in accounting that night
Because Tom in accounting was promoted
And Bob thought that just wasn't right

So while the company focused on China,
And tried to work out why Iran was involved
And spent lots of money on vendors
The incident could have been solved…

By taking a look at what happened
Not jumping the gun to decide
That malware was the root of the problem
While Bob got away with his crime.

by Shane Shook, PhD
https://blogs.blackberry.com/en/2013/07/green-eggs-and-spam-efficient-incident-response

The Concept of "CIBOK"

What is the Reason for CIBOK?

Cybersecurity is a function of Information Technology (IT) which seeks to identify and mitigate cyber risks to the organization. The organization has operating risks and related controls that are managed by policies, procedures, and training – and are supported by IT for information collection, processing, management, retention, and protection. IT also supports the risk management function of the organization to mitigate risks to the organization' s ability to continuously serve customers (downstream) and to satisfy executive management in their obligations to the market, shareholders, and partners.

As IT has evolved to support organizational requirements, related evolutions in methods to leverage technology as a tool, to target IT used by a company, and to disrupt or distract organizational functions through cyber means have occurred. The Chief Information Officer (CIO) has gained a seat at the boardroom table to participate in organizational strategy, with responsibilities to ensure the continuity of operations through IT support, including information protection and infrastructure security. To support the CIO, the Chief Information Officer (CISO) role has been created to oversee strategic and tactical planning along with resource management.

The rapid advance of IT and correlated threats has simultaneously created new skill, knowledge, and experience requirements as market intelligence (open source and proprietary) has evolved to create new risks to the organization. As a result, in order to support the investigative and intelligence needs of the organization, the Cybercrime Investigator role has emerged. The Cybercrime Investigative Body of Knowledge (CIBOK) is intended to describe the skills, background, and requirements for cybercrime investigators to assist law enforcement and corporate risk managers (and IT).

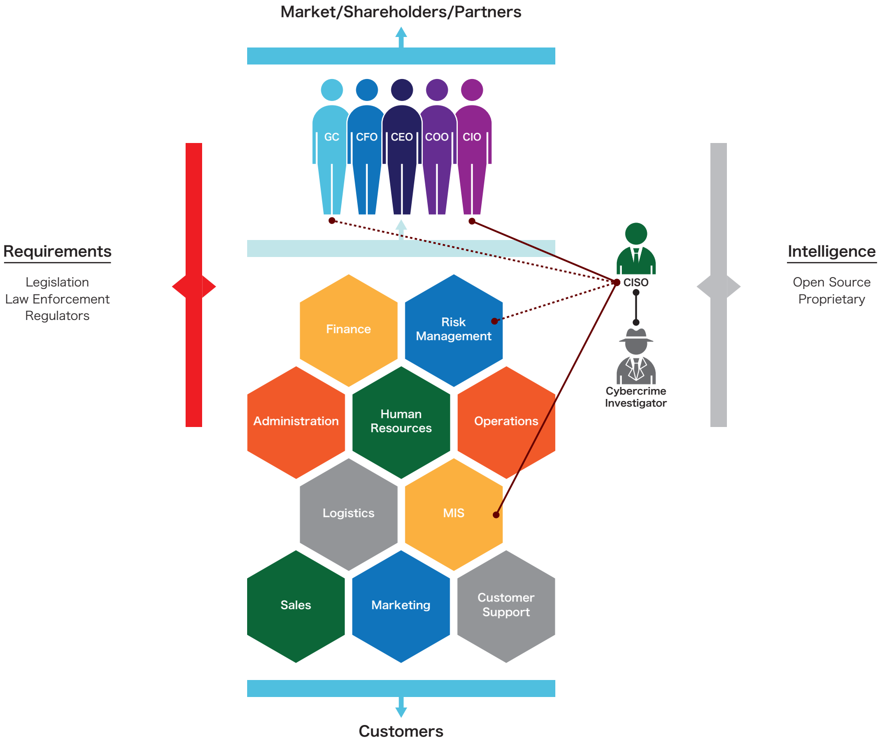


Figure 1-1. Cybercrime Investigation Function

The Objective of “CIBOK”

What is the Objective of this Document?

The objective of the CIBOK is to demonstrate best practices that capable and skillful cybercrime investigators implement in their investigative activities.

The purpose is to demonstrate an accessible taxonomy - a systematic classification and organization of the knowledge, skills, and approaches that must be commonly mastered in cybercrime investigations. To this end, descriptions concerning each topic are limited to only the necessary scope for the reader to successfully discover reference materials related to the topic. The body of knowledge itself is not found within this document, but can be discovered from the reference materials.

The Five Objectives of CIBOK Establishment

This document has been created in accordance with the following five objectives:

1. Popularizing and promoting a commonsense approach to consistent cybercrime investigations throughout the entire world, independent of the laws in each country.
2. Providing a detailed demonstration of other systematized customary practices in project management, computer science, and digital forensics within the scope of cybercrime investigations.
3. Characterizing and demonstrating content that should be put into practice in cybercrime investigations.
4. Presenting means to utilize topics in practice.
5. Demonstrating that cybercrime investigative training curricula development and individual knowledge and skills are of a high level.

In order to achieve the first objective (knowledge concerning consistent worldwide cybercrime investigations), this document has been created with the participation of authors from around the world (including reviewers).

In order to achieve the second objective (detailed demonstration of other systemized customary practices within the scope of cybercrime investigations), certain materials have been included as executable frameworks; these materials are classified in accordance with the cybercrime investigations execution framework (which is composed of the eight knowledge areas exemplified in figure 1-2).

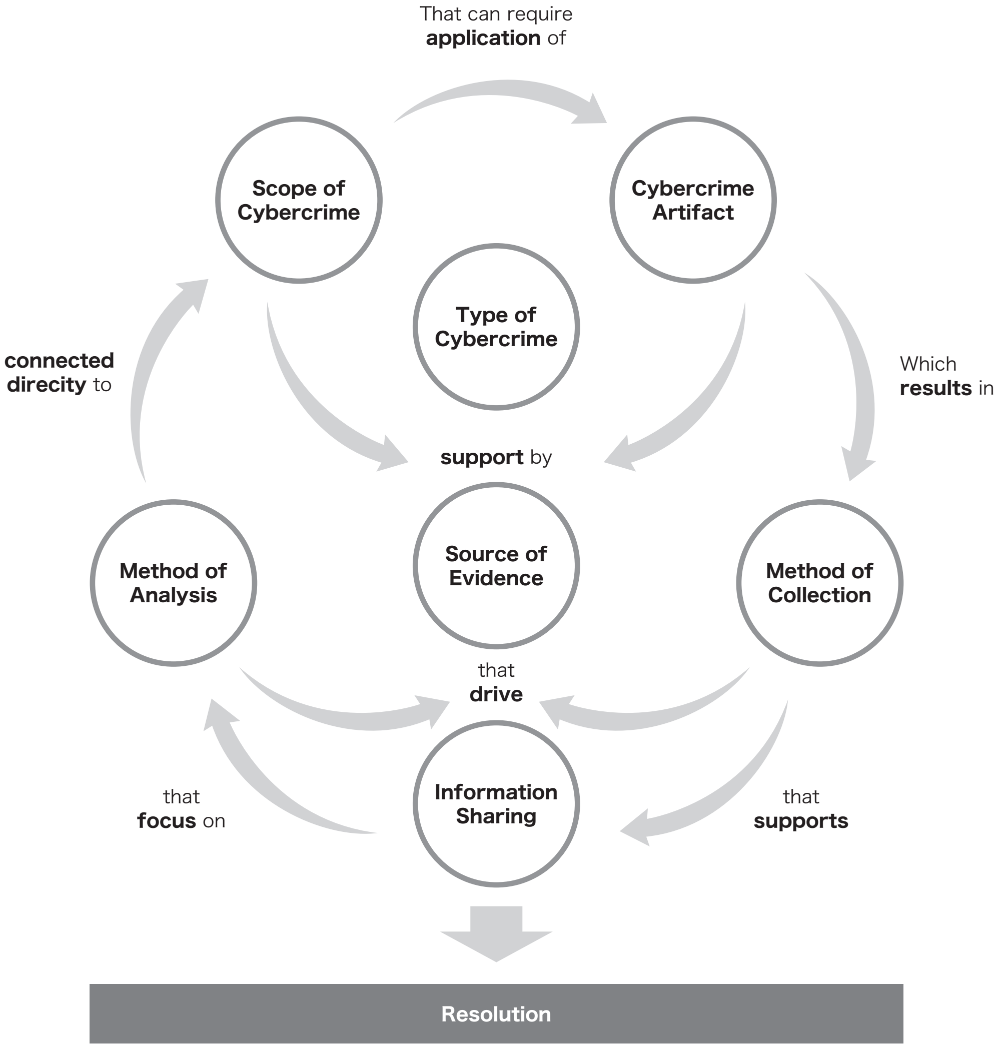


Figure 1-2. Cybercrime Investigation Execution Framework

When detailing the scope, it is important to identify cybercrime investigations and intersecting work practices. In this document, intersecting areas are presented using the six frameworks exemplified in table 1-1. The acquisition of comprehensive knowledge in these related frameworks is required for effective work practices but falls outside of this document' s scope.

For example, the knowledge and skills required for all new police officers (regardless of whether they are in the cyber field) are defined as "police officer core" frameworks. These can be learned by fulfilling official requirements for police officers stipulated by the legislative system of each country.

This document considers police officer core frameworks as prerequisites and as such does not refer to them. 13 knowledge areas which compose these frameworks are provided below as reference information. Please note that knowledge areas differ according to the legislative system of each country. To acquire core frameworks, official certification is carried out through training at police academies or other training and development institutions, and typically includes 600-1000 hours of testing.

Table 1-1. “Related” Frameworks that Support “Practical Implementation”

Framework Name	Knowledge Area
Criminal Policy Strategy & Governance Framework	The scope of this framework includes corrections policy and victimology, and its purpose is to ensure that, police organizations, in order to define and plan strategies for the execution of criminal policy connected with criminal law in the cyber field, have been operating soundly and effectively.
Funding & Budgeting Management Framework	The purpose of this framework is to clarify the financial functions necessary to support the implementation of a criminal strategy and, by appropriately controlling annual expenditure, to allocate limited funds and resources efficiently in respect of the measures that are deemed to be necessary, to achieve results reliably and effectively.
Effective Policing & Crime Prevention Management Framework	In relation to the mission of “maintaining order” , within which it is hard to prioritize, the purpose of this framework is to consider what provision of high-quality “Policing Services” can satisfy stakeholder requirements and achieve social results.
Cybercrime Investigation Execution Framework	Type of cybercrime
	Cybercrime Artifact
	Scope of Cybercrime
	Source of Evidence
	Method of Collection
	Method of Analysis
	Information Sharing
	Resolution
Foundations	Computer Engineering
	Computer Science
	System Engineering
	Project Management
Police Officer Core	Administrative Procedures
	Constitutional Law
	Ethics and Professionalism
	Human Behavior
	Policing and Patrol
	Homeland Security
	Law Enforcement
	Criminal Investigation
	Report Writing
	First Responder
	Defensive Tactics
	Firearms
	Physical Training and Wellbeing

These six frameworks investigative divisions contributing to cybercrime investigations use to manage cybercrime departments form a “**macro framework**” as shown in figure 1-3.

In the chapters of this document, macro frameworks are analyzed and defined at a micro level, displaying the main activities and procedures investigators must learn to measure the effects that daily cybercrime investigation activities have on criminal policy.

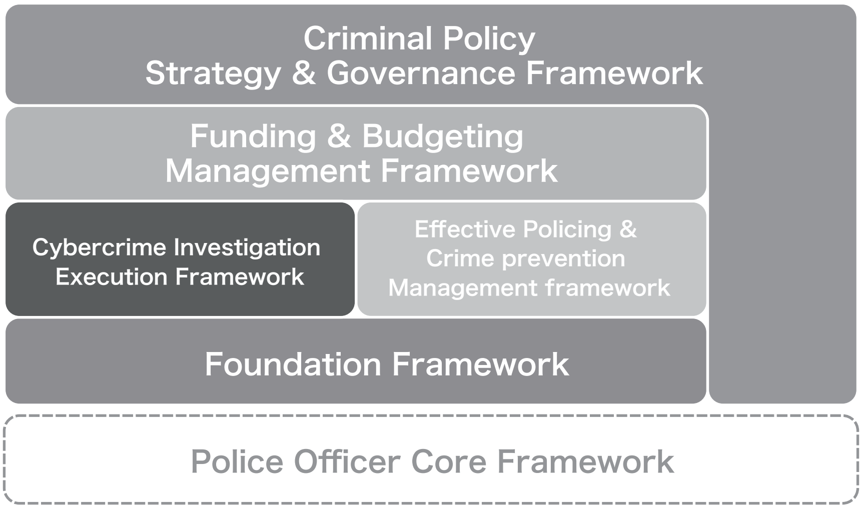


Figure 1-3. Macro Framework of Cybercrime Investigative Divisions

In order to achieve the third objective (characterizing and demonstrating content that should be put into practice in cybercrime investigations), the organizational structures of each knowledge area are classified.

In order to achieve the fourth objective (presenting means to utilize topics in practice), this document provides respected reference material in each of the eight knowledge areas (shown in Figure 1-2) along with two chapters (Chapters 10 and 11, respectively) that present a management framework and an approach to practical cyber risk management.

In order to achieve the fifth objective (demonstrating that cybercrime investigative training curricula development and individual knowledge and skills are of a high level), this document examines the knowledge and skills currently used by investigators engaging in the investigation of cybercrime, collated as an analysis of duties. By doing so, commonly accepted knowledge standards are established and investigators' capabilities can be evaluated using objective and reliable methods such as standards-based note taking, verbal statements, practical skill assessments, and observation.

Cybercrime and its Investigation

What is Cybercrime?

What the law stipulates as a crime differs from country to country; this is not limited to the cyber field. Furthermore, what should be considered a crime changes in accordance with historical context. Consequently, this document defines "**cybercrime**" as follows:

> Cybercrime is defined as acts involving **cyber space** (including computers, computer software, computer networks, or embedded software controlling systems) which violate various strongly defined norms in society's collective consciousness

Cyberspace is a new **social area** which consists of networks. This area already permeates all corners of civic life, and the number of other areas that can use cyberspace is expanding on a regional and global scale. Cyberspace provides essential infrastructure supporting a variety of activities in actual "areas" including land, sea, air, and space. As with areas outside the jurisdiction of nations (international waters, international airspace, etc.), it can be perceived as a shared asset of humanity, and as a result criminal activities in cyberspace differ from conventional crimes.

The criminal elements that should be considered in "**Criminology**" or "**criminal policy**" are presented in figure 1-4 using "**b/d/r dynamics**":

> Crime is when an "**individual**" commits harmful "**behavior**" which "**damages**" a "**victim**", and a "**reaction**" from "**society**" occurs in response.

I – b・d – V
r
|
S

Figure 1-4. b/d/r Dynamics

As shown in figure 1-4, the "reaction" differs in accordance with the country which composes the "society". Consequently, it is inevitable that the definition of crime will differ by country. Furthermore, in criminal investigations it is necessary to refine the target of the investigation not only by the "behavior" but also by the "damage". On top of this, the individual must be discovered and evidence must be secured through investigation.

There are instances in which misappropriation and misdeeds in cyberspace are used simply as the means to realize criminal acts already defined by law. It is essential for law enforcement agencies to quickly ascertain whether coordination with conventional investigative branches will accelerate investigations into these harmful behaviors. Therefore, the categories of harmful behavior occurring in cyberspace must be defined, as shown in table 1-2:

Table 1-2. Categories of Harmful Behaviors Occurring in Cyberspace

Technology as Target	Behavior that could not have existed before the arrival of cyberspace which damages a victim.
Technology as Instrument	Behavior which damages a victim through misuse of cyberspace or its technologies.
Technology as a Distraction	Behavior that is intended to obscure criminal objectives by distracting investigators and responders away from targeted systems or information.
Technology Is Incidental to Other Crimes	Money laundering and unlawful banking transactions, organized crime records or books, and bookmaking.
Crime Associated with the Prevalence of Technology	Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment.

Tables 1-3 and 1-4 categorize damages and risks to victims from harmful behaviors occurring in cyberspace.

Table 1-3. Categories of Damages to Victims Caused by Harmful Behaviors Occurring in Cyberspace

Bodily damage	Property damage	Passive damage	Costs required to respond to incidents arising due to receiving a cyberattack and restitution for responsibility
		Active damage	Lost profits and costs of continuing business arising from non-functioning IT equipment etc. as a result of receiving a cyberattack, or damages regarding lost market opportunities
	Psychological damage	Damage from suffering (defamation, loss of trust) at having received a cyberattack	

Table 1-4. Categories of Risks to Victims in Cyberspace

Category name	Details
Availability risk	Damage caused by downed systems etc.
Performance risk	Damage caused by lowered system processing capabilities
Market risk	Damage caused by brand devaluation or loss of market confidence
Fraud risk	Damage caused by theft or manipulation of financial or securities-related protected information
Compliance risk	Damage caused by lack of compliance with laws and guidelines
Security risk	Damage caused by inadequate security countermeasures
Safety risk	Damage caused by systems manipulation that endanger personnel

What are Cybercrime Investigations?

This document defines "**cybercrime investigations**" as follows:

> Acts involving the discovery, collection, preservation, and securing of criminal evidence in order to file and maintain a prosecution when a crime is deemed to have taken place in cyberspace

These activities can be generally classified into two categories as shown in table 1-5- “**proactive investigations**" and “**reactive investigations**”:

Table 1-5. Categories of Cybercrime Investigation Activities

Proactive investigation	Investigation activities in which law enforcement agencies envision suspects who are planning crimes and make arrests for that objective. In this type of operation, building "**intelligence**" is the first step in the activity.
Reactive investigation	Activities performed after a crime has occurred in which law enforcement agencies collect and secure proof regarding the suspect and make arrests for that objective. In this type of investigation, "**reports**" from citizens or "**patrols**" by investigators are the first step in the activity.

The essence of cybercrime investigation activities is the same as traditional investigation activities. In both types of investigation activities, investigators must comply with the laws, regulations, and conventions of each associated country. Furthermore, in the investigation activities it is essential to use investigative powers honestly and fairly to establish facts and resolve the matter without unjustly violating personal freedoms and rights.

However, cyber crimes do have some characteristics which differ from traditional crimes, as shown in table 1-6:

Table 1-6. Characteristics of Crime in Cyberspace

1. No time or geographic restrictions	Cyberspace is a social area connected by networks. As a result, synchronous and asynchronous exchanges which are not restricted by the geographic location (location where a crime is committed, location of evidence, location where damage occurs) of physical whereabouts are possible.
2. Damage in unspecified large numbers	In cyberspace, it is possible to send information to an unspecified large number of people, and it is easy to affect an unspecified large number of people within a short period of time.
3. No traceability	In cyberspace, all exchanges are conducted with digital data. Unless specific measures to preserve that data are taken, no trace will exist. In addition, even in the event that the data is recorded, alteration, deletion, encryption and obfuscation are easy.
4. Anonymity	In cyberspace, it is easy to impersonate another party' s face or voice, and there are no physical traces such as handwriting, fingerprints, etc. Verification of whether or not the other party is the person that he/she claims to be is dependent on digital data.

Due to these characteristics, investigation activities require reform in all segments when involving cybercrime. Two key aspects are presented here.

The first aspect is cooperation and coordination in cybercrime investigation activities. Most traditional crime is carried out within one jurisdiction. Because of this, related investigation activities have been built on the premise that the criminal and victim exist within the same territory. Cyberspace has brought about the diversification of individual existences and corporate economic activities, and continues to break down a number of boundaries that were traditionally thought of as a matter of course (such as the framework of the nation-state). These changes have caused criminal investigation activities to become more difficult. For example, there are instances in which a criminal has immediately fled to a new jurisdiction after committing a crime, as well as instances in which the same criminal commits successive crimes over a wide area.

In addition, the organizational capacity of **organized crime groups** has risen as they use cyberspace as infrastructure to increase their international activities and move into foreign countries. Furthermore, emergent organized crime groups dealing in new types of cybercrimes that target technologies have appeared ("Technology as Target", as shown in table 1-2).

As a result, cybercrime investigations presuppose activities that constantly straddle multiple jurisdictions. In order for initial measures taken after an incident to be fast and accurate, it is essential to form "**wide area investigation units**" which conduct investigations that cross units of police jurisdiction. Adjustment and coordination between international sovereignties must also be given attention.

The second aspect is the "**destruction of evidence**" by the criminal during the cybercrime investigation activities. It is difficult to carry out prosecution and maintain a public trial unless there is admissible evidence acquired through lawful means. For cybercrime in particular, limits are placed on obtainable evidence through external "**verification**" implemented via a core investigative agency. Because all actions in cyberspace are exchanges of digital data, unless specific measures to preserve that data are taken no trace will exist. Moreover, there is evidence that can only be obtained using an internal "**expert opinion**" given by a person with specialist knowledge.

As a consequence, investigators who are engaging in cybercrime investigations must avoid preconceptions and eliminate baseless conjecture. They must handle not only the tangible objects which can be "**physical evidence**", but digital evidence as well. They should not overestimate "**witness testimony**" from suspects and other related parties. In cyberspace, conflicts can occur through misunderstanding and assumptions. Basic investigations must be thoroughly implemented in a logical manner, striving for the discovery and collection of all evidence.

When carrying out an investigation, overall judgments must be made based on all available information and collated materials. This requires the practical application of extensive knowledge and technical skills. However, investigators should not overestimate their own abilities or rely solely on their own judgments. It is essential that they are constantly aware of an investigator's ethics and advance investigations comprehensively through organizational strengths.

Strategy and Planning Based on Criminal Policy

Framework for Value Creation

The ultimate success for cybercrime investigative divisions in law enforcement agencies is "**mission**" accomplishment. Figure 1-5 presents a framework for deriving strategies from missions.

The "mission" (the most important long-term objective) increases the satisfaction of "**stakeholders**" by providing quality police services. Consequently, the mission is positioned at the top of the framework displayed in figure 1-5.

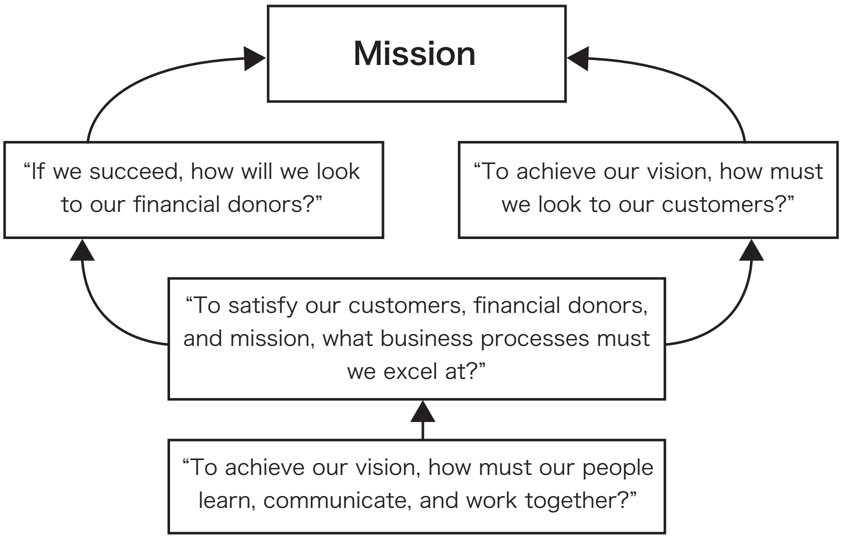

Mission
"If we succeed, how will we look to our financial donors?"
"To achieve our vision, how must we look to our customers?"
"To satisfy our customers, financial donors, and mission, what business processes must we excel at?"
"To achieve our vision, how must our people learn, communicate, and work together?"

Figure 1-5. Adapting the Framework to Cybercrime Investigation Unit

The missions that law enforcement agencies brandish are wide and diverse. For example, the mission of "**INTERPOL**" states the following:

Preventing and fighting crime through enhanced cooperation and innovation on police and security matters

The missions of INTERPOL and other law enforcement agencies include content with lofty social significance such as "**maintain order**". As a result, the achievement criteria are social indicators which can be difficult to order by priority.

To plan the conditions to achieve missions, first consider the "**customer perspective**": what stakeholders require of "**cybercrime units**" and the kinds of quality of "**policing services**" that fulfill their demands and attain social achievements.

- Stakeholder definition (investigators, taxpayers, donors, police commissioners, parliament, cooperating private corporations, etc.)
- Stakeholder segmentation
- What should be offered to stakeholders?

- How can the opinions of stakeholders be ascertained and fed into strategies?

The strategic objectives of important stakeholders such as taxpayers and donors are reflected in "**consignee viewpoints**". Unlike customers, donors are not necessarily the beneficiaries of police services. They may become service beneficiaries but often do not.

The framework displayed in figure 1-4 indicates the route to success for law enforcement agencies through the performance of "**viewpoints of internal processes**" supported by "**viewpoints of learning and growth**".

The resources used by law enforcement agencies are by no means inexhaustible. Resources are reliant on provisions from stakeholders such as investigators, taxpayers, donors, police commissioners, parliament, and cooperating private corporations. However, financial criteria are not necessarily adequate indicators of whether agencies are fulfilling their missions. Unless there is a clear relationship between social indicators and financial indicators, financial viewpoints should not be included in frameworks for deriving strategies from missions.

Composition of Cybercrime Investigative Divisions

Considerations of Cyber Divisions in the Structures of Traditional Investigation Organizations

Figure 1-6 shows the structure of a basic traditional crime investigation organization. Cybercrime investigators must provide police services for traditional organizational structures in accordance with the demands of society or organizations.

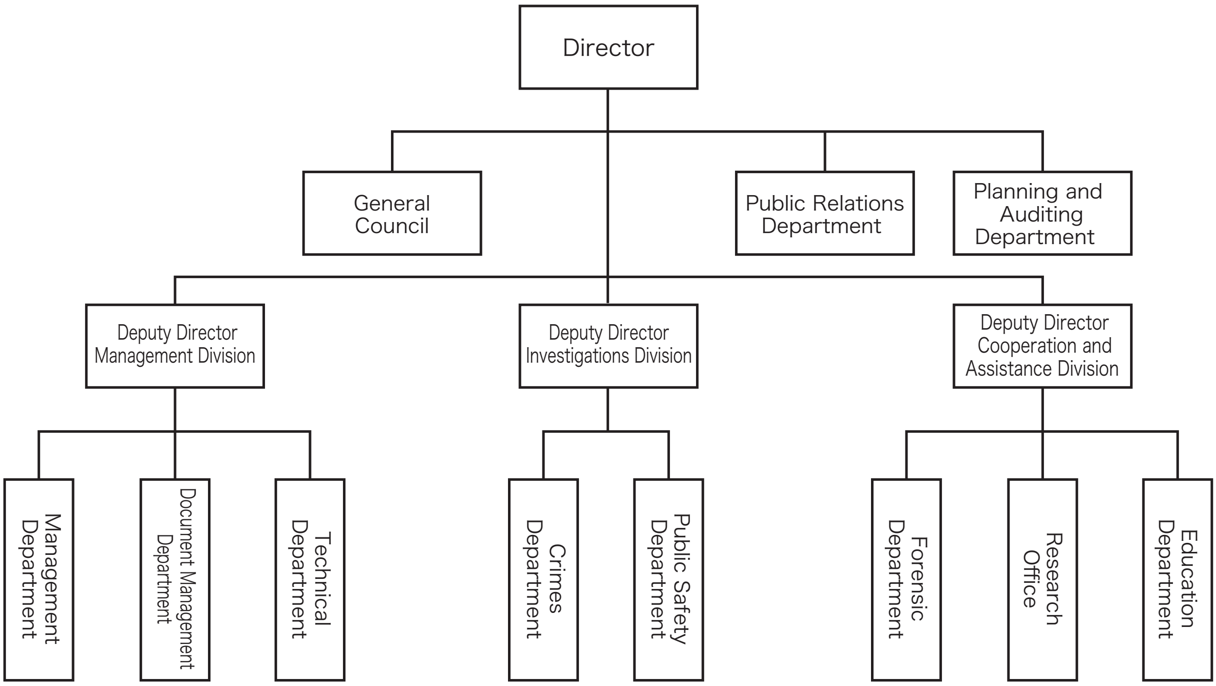

Director
General Council
Public Relations Department
Planning and Auditing Department
Deputy Director Management Division
Deputy Director Investigations Division
Deputy Director Cooperation and Assistance Division
Management Department
Document Management Department
Technical Department
Crimes Department
Public Safety Department
Forensic Department
Research Office
Education Department

Figure 1-6. Structure of a Basic Traditional Crime Investigation Organization

Cyber divisions and cyber investigators must be able to coordinate with conventional investigative divisions to resolve incidents.

The director is responsible for commanding the duties performed by the "**cybercrime unit**". This post differs according to the form of the organization. Here, this person is defined as the "commander" for purposes of convenience.

The authority, resources, and personnel afforded to the commander will differ depending on the organizational structure. However, in all cases it is essential for the commander to achieve high-quality communication with the head of the organization.

The breadth of the organizational structure will depend on its scope as stipulated by the organization's head, the commander, or by law.

The "**category-type organization**" presented in figure 1-7 is an example of an organization divided into specialist "departments" such as the Crimes Department and Public Safety Department, which are subordinate to "divisions". These departments are divided into "sections" which focus on categories of crimes (felonies, drugs, firearms, fraud, etc.). Cybercrime units are placed under these sections as organizations controlled by the commander. The legislative systems of each country should be referred to when categorizing these departments and sections.

In a category-type organizational structure, the scope of the cybercrime unit' s responsibilities is limited to category division areas. Consequently, units can start up with few personnel. As figure 1-7 shows, some are joint units in multiple sections while others exclusive units for specific sections. In either case, since units have a limited scope, multiple sections may simultaneously request the establishment of units responsible for similar functions . In the event that units responsible for similar functions are dispersed, communication across those units will be an issue.

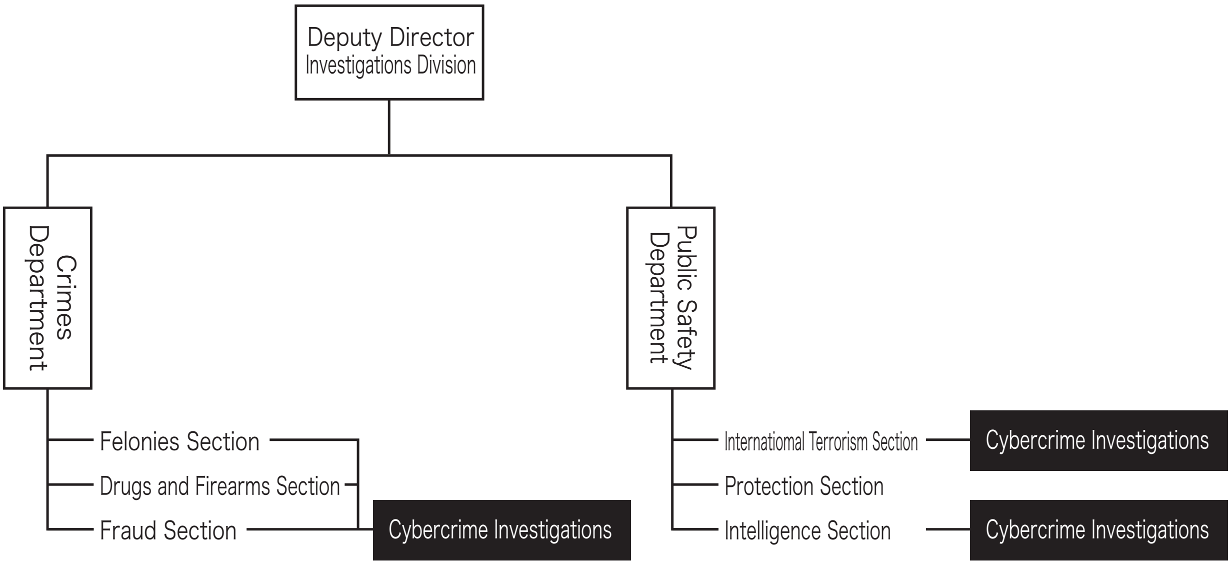


Figure 1-7. Category-type Organizations

As shown in figure 1-8, in “**matrix-type organizations**” cybercrime investigation units are established as specialist “departments”. Cybercrime units are placed under departments as organizations controlled by the commander.

In matrix-type organizations, the scope of a unit's responsibilities expands to all departmental areas. Consequently, it is necessary to retain stronger powers, resources, and personnel. In addition, personnel appointed as a department' s contact for interdepartmental liaison should have expertise in their department. In figure 1-7, these units are illustrated as subordinate organizations of the “Cooperation and Assistance Division” ,but they may also be subordinate organizations of the “Investigative Division” in some cases. Consider the legislative system of each country and each division' s scope when deciding where to locate cybercrime units.

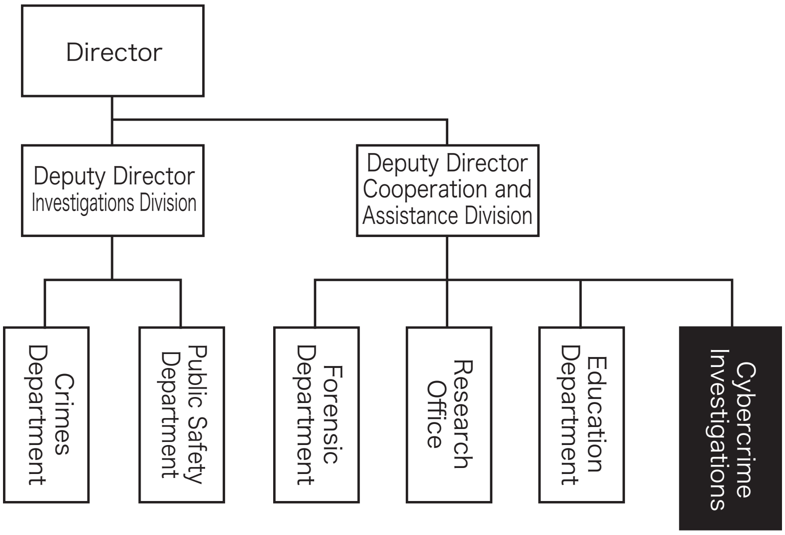


Figure 1-8. Matrix-type Organizations

The "**composite-type organizations**" exemplified in figure 1-9 are a combination of category-type and matrix structures. Cybercrime investigation units exist both as specialist departments and as organizations under departmental sections.

In composite-type organizations, it is possible to adjust the scope of unit responsibilities. During normal times, units may act as category-type organizations; in emergencies, project teams may be composed separately and a separate commander may be appointed.

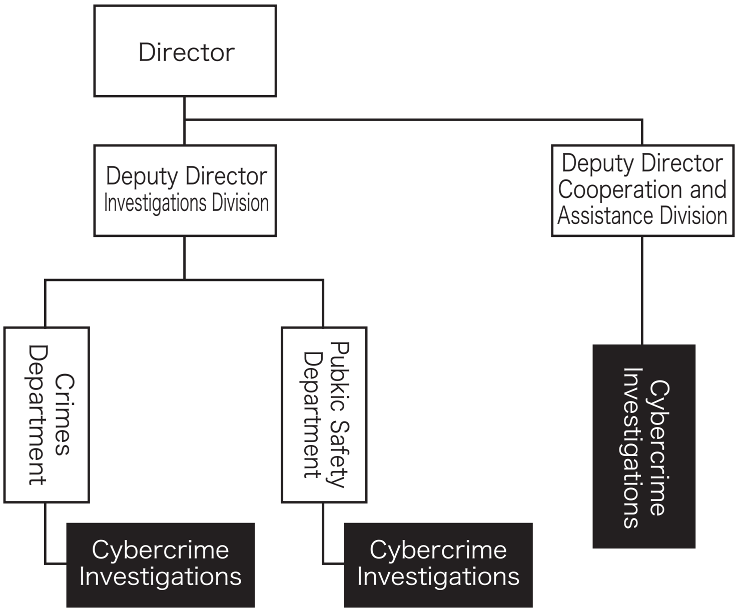


Figure 1-9. Composite-type Organizations

Cybercrime investigation units achieve success by providing services to traditional organizational systems and cooperating with other units to promote mutual understanding and functionality. Communication between members and divisions across areas is an essential aspect of cybercrime investigations.

In all organizational structures, mutual exchange regarding the following primary factors must occur:

- The strategic importance of the cybercrime investigation
- The maturity of the cybercrime investigation
- The management system of the cybercrime investigation

In response to the increase in international cybercrime, law enforcement agencies and private companies must be prepared for public-private collaboration, efficient communication, and the use of external resources. Currently, collaboration between investigative agencies and private companies is dominated by a technology-driven approach. In order to strengthen this collaboration and enable effective management, corporate executive leaders must oversee the development of corporate risk management capabilities.

Chapter 10 and Chapter 11 (new in this edition) introduce and apply a management framework for businesses establishing appropriate information and security capabilities, covering the following topics:

- Deepening the understanding of challenges related to cybercrime and information governance as international issues, and exploring appropriate countermeasures.
- Clarifying the division of responsibilities between the organization's integrity and IT departments, and responding to governance issues.
- Aligning with business strategies and appropriately prioritizing and allocating resources for security activities and risks.
- Sharing common values in security responses and supply chain management, and maintaining consistent governance.
- Establishing a flexible framework to set realistic standards in the rapidly evolving cybersecurity landscape.

The corporate cyber risk management framework helps companies overcome barriers resulting from the varied expectations, laws, and other practices around cyber crimes in different countries, in order to better cooperate with law enforcement agencies. The implementation of this framework enables companies to respond more effectively to cybercrimes and better contribute to the maintenance of security and prosperity in the international community. Table 1-9 shows the comprehensive CIBOK taxonomy, including the management framework, and its relationship to Strategic, Tactical, and Procedural knowledge domains.

Cybercrime Investigations

Figure 1-10 shows the structure of a typical cybercrime investigations unit. The structure will change depending on each country' s laws, the cooperating organizations, personnel serving concurrent posts, and other factors. The functional systems and personnel required for cybercrime investigation units are clarified here.

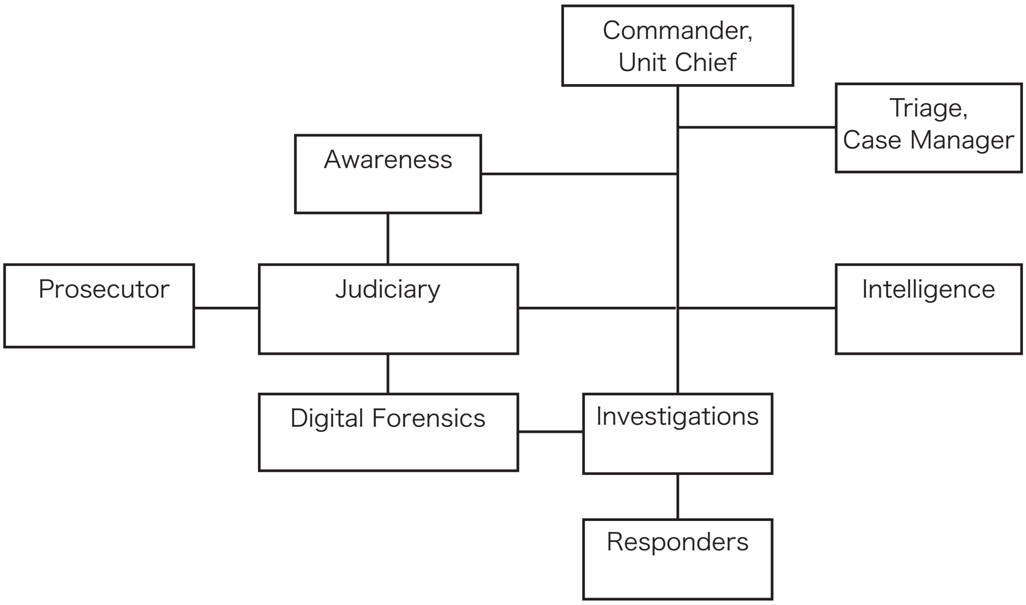


Figure 1-10. Structural Diagram of a Cybercrime Investigations Unit

Typical cybercrime investigations units include a number of specialists. If personnel with appropriate "**capabilities**" and skills cannot be secured immediately, appropriate consideration should be given to requesting personnel from outside the organization. Moreover, consideration should be given to staff training.

The content of duties will differ depending on the specialist. However, the unit should always be formed for the purpose of achieving a common mission. Consequently, specialist areas and responsibilities should be clarified and contribute to the cybercrime investigation unit' s mission. The following specialist areas are common in cybercrime investigations units:

1. Management/Executive (Commander, Unit Chief, Triage, Case Manager)
2. Intelligence
3. Investigations
   a. Responders
   b. Digital Forensics
4. Judiciary
5. Public Relation, Awareness
6. Support
7. Administrative

Management

Management refers to investigators with decision-making responsibilities who coordinate with related stakeholders in complex incident investigations.

In this function, investigators formulate plans for activities concerning cybercrime investigations and manage personnel based on medium-term forecasts. Since management understands the expectations and abilities of cybercrime investigation units within crime investigation organizations, this specialist area is able to decide what kind of information, tools, and training should be provided to cybercrime investigators.

Furthermore, management is able to share information concerning inter-field cybercrime and cyberattacks with external shareholders.

For separate cybercrimes, Management judges how to engage, prioritize, and allocate personnel and resources across multiple cybercrime investigations from a comprehensive point of view and is responsible for case managers and triage functions.

In addition, crime trend vectors in cybercrime are becoming more advanced and diverse, expanding "from country to country", "from large organizations to small organizations", and "between similar industries"; management can understand these trends and promote relevant information sharing.

The CIBOK refers to "Managers" as an "Executive" activity in the taxonomy.

Intelligence

Intelligence refers to investigators responsible for considering effective investigative strategies and asset allocation by perceiving overall directions and trends, using a variety of information.

This function performs statistical processing (data retrieval, collection, extraction, cleanup, analysis, and modeling) of cybercrime predictions and data reported by analysts. Intelligence investigators have knowledge and technical skills which allow them to build operation intelligence from a variety of sources (economic environment, macro/micro economics, etc.) that can be used in criminal investigations.

In normal times, this function can expand the scope of information collection and apply standardized data structures and models to collected data in order to build a data management system for archival purposes.

Investigations

Investigations refers to investigators who handle a variety of cyber matters for police organizations. This function requires research knowledge and skills.

These investigators are well versed in the technical aspects of cybercrime, have a good command of computer science and network investigations, and are able to provide information enabling the arrest of offenders by coordinating with other investigators.

In normal times, this function supports the development of training programs for junior levels or incident response investigators and can develop cybercrime awareness training for the public .

Responders

Responders are investigators responsible for investigative patrols in cyberspace aimed at maintaining order.

This function has a good command of technical knowledge. Responders make the first response, visit crime scenes first, and report crimes. At crime scenes, responders specify what "digital evidence" is available and ascertain the potential effects of that evidence. Responders' reports help management decide the order of priority across different investigations.

Digital Forensics

Digital forensics refers to investigators responsible for collecting and recovering "digital evidence" from physical digital equipment in cybercrime incidents.

This function requires a fundamental background in computer science and network investigations. Digital forensics investigators must have knowledge and skills concerning "computer forensics principles" and be able to identify "digital evidence".

This function attempts to restore evidence that has been obfuscated by alteration, deletion, or encryption. by the suspect.

At the hearing stage, this function also supports investigators in the judiciary function by drafting written questions or providing relevant data submissions.

Judiciary

Judiciary investigators are responsible for preparing foundational material by arranging "digital evidence" from perspectives of -means, admissibility, and probative value on the basis of substantive law and procedural law. This role oversees accountability in police procedures concerning cybercrime and understands substantive and procedural law concerning police investigations. Judiciary investigators also require knowledge and technical skills at a level equivalent to investigators responsible for "digital forensics" and "investigations".

In wide investigations requiring coordination between international dominions, judiciary investigators can link with other regional judiciary investigators who are well acquainted with the circumstances.

Public Relation and Awareness

Public relations and awareness investigators are responsible for cybercrime prevention initiatives.

In this function, investigators analyze the opportunities that enabled cybercrime. These investigators require knowledge and skills to provide cybercrime prevention information to improve public awareness based on crime prevention environment plans.

This function formulates effective crime prevention measures tailored to the actual state of cybercrime by coordinating with investigations and judiciary investigators. These investigators are also able to promote public relations and awareness, educational opportunities, and information sharing to facilitate thought reform among blue-collar workers, entrepreneurs, and regional populations while linking with national governments and interested bodies.

Support

This function includes IT and facilities support activities specific to the services provided.

Administrative

This function includes clerical, human resources, budget control, and related activities specific to the services provided.

Each of these functions has distinct relationships to the "Execution Frameworks for Cybercrime Investigations". For each framework, the level of skills and experience required by each function is described as "**H**igh", "**M**edium", and "**L**ow" (or "**N**ot/**A**pplicable"), as demonstrated in table 1-7. Note that "Cybercrime Investigation" and "Management" are program activities not to be confused with functions performing those activities.

High = detailed understanding and practical experience developing and interpreting policy and procedures concerning the knowledge domain.

Medium = knowledge and experience gained through application and management of others who utilize policy, procedures, and related technology in the associated knowledge domain.

Low = ability to apply knowledge and skills to meet policy requirements, follow related procedural guidance, and utilize associated technology in the knowledge domain.

N/A = does not apply to the function in the associated knowledge domain.

In addition, for each framework, related knowledge domains used by each function are described as Strategic (planned long term goals), **T**actical (planned incidental or response activities), and **P**rocedural (activities supported by procedures, tools, and testing), as demonstrated in table 1-8.

Table 1-7. Relationships between CI Execution Frameworks and CI Role required skills and experience.

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Table 1-8. Association of CI Execution Frameworks to CI Role knowledge domains.

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Table 1-9. CIBOK Taxonomy

Strategic Knowledge, Skills and Experience														
		Tactical Knowledge, Skills and Experience												
					Procedural Knowledge, Skills and Experience									
Cybercrime Investigation	Description of Cybercrime	Objectives of Cybercrime	Cybercriminal Profiles	Cybercriminal Organizations	Indicators	Stages	Artifacts	Scope	Sources of Evidence	Methods of Evidence Collection	Methods of Evidence Analysis	Resolution	Cybercrime Information Sharing	Management Framework
Laws	Tool	Subversion	Anti-societal	Hackers	Attack	Targeting	The Internet	Incidental	OSINT	Automated	Collection	Organization	Classification	Strategy & Governance
Jurisdictions and Policies	Target	Sabotage	Extortionist	Service Providers	Reconnaissance	Access Provisioning	Deep Web	Targeted	PROPINT	Manual	Aggregation	Communications	Authority	Planning & Budgeting
Best Practices	Distraction	Theft/Fraud	Destructive	Service Subscribers	Compromise	Cataloguing	Dark Web	Evolved	Forums	Procedures	Association	Technical Remediation	Notification	Human Resources
		Espionage	Anarchist	Perpetrators	Exploitation	Service Definition	Social Media	Financial	Botnet Control Panels	Requirements by Type	Data Model	Procedural Remediation	Venues	Performance Management
			Thief			Service Administration	Criminal Networks	Brand	Networks	Requirements by Category	ETL			People Management
			Spy			Service Support/ Defense	Traditional Media	Operations	Hosts		Data Quality			Tool Management
						Redundancy of Services	Systems	Personnel	Services		Automation			
						Obfuscation	Personnel	Public Organization			QA/QC			
						Alternate Services	Communications	Private Organization			Analysis			
						Attainment of Objectives					Interpretation			
											Second-Party Review			

Chapter 1

Cybercrime and its Investigation

Introduction

Crimes have always been a factor in society. Crimes are committed for varied reasons and may be committed to support associated purposes. The impact of a criminal act is interpreted by society to merit reasonable penalties.

Crimes are committed by humans who utilize tools to facilitate their activities. Cybercrimes are committed by humans who use computers for those purposes.

Before businesses were connected by networks or the Internet, intrusions were performed with hammers, lock picks, stolen badges or alarm system codes, or broken windows. Today' s business intruders use spear phishing emails, SQL injection attacks on web services, and social engineering techniques. The crime is the same –breaking and entering- but the tools used to achieve that objective are different. At the end of the day, a crime is still committed by a person.

Although cybercrimes have evolved since 2014, they still intend to achieve objective outcomes that benefit the criminal at the expense of the victim. These crimes can range from stealing sensitive information, such as personal or financial data, to disrupting or otherwise sabotaging computer systems (and data).

In today's digital age, businesses of all sizes are at risk of falling victim to cybercrimes. According to a 2013 study conducted by the U.S. National Small Business Association, 44% of small businesses had experienced a cyber attack and the average cost for these attacks was $9,000 per incident[1]. By 2016 that figure had risen to 50%, with 60% of those victim companies subsequently having gone out of business. As of 2023, the global average cost per data breach was $4.45 million U.S. dollars[2].

It' s not just financial losses that businesses need to worry about. Cybercrimes can also damage a company' s reputation and erode customer trust. Cybercrimes can also result in physical damages to systems and even to people. A 2023 study[3] of ransomware attacks on U.S. hospitals suggested that between 2016-2021 up to 67 Medicare patients died due to damage caused by those attacks. This is a chilling reminder of why it' s so important for companies to take steps to protect themselves from cyber threats.

Education and awareness are crucial measures to protect against cybercrimes. Companies must prioritize these to safeguard their interests. They should educate employees not only on "best" security practices, but indeed upon what constitutes a cybercrime. This might involve highlighting potential risks such as phishing emails or malware attacks, and providing examples of these types of cybercrimes to help employees identify and prevent them. It' s also important for companies to regularly review and update their security protocols and systems to stay ahead of evolving cyber threats.

Another important aspect in preventing cybercrimes is creating a culture of cybersecurity within the company. This means fostering a mindset where all employees are responsible for maintaining the security of the company' s (dependency on) technology and related information.

[1] https://www.prnewswire.com/news-releases/nsba-economic-report-small-business-outlook-vastly-improved-300037112.html

[2] https://www.statista.com/statistics/987474/global-average-cost-data-breach/

[3] McGlave, Claire and Neprash, Hannah and Nikpay, Sayeh, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). Available at SSRN: https://ssrn.com/abstract=4579292 or http://dx.doi.org/10.2139/ssrn.4579292

This chapter will explore the legal principles that relate to cybercrimes and how cybercrimes are defined, investigated, and prosecuted. It will also review issues of self-governance as well as jurisdictional guidance (and constraints) that factor into the methods of investigation and prosecution. The roles and responsibilities of organizational and investigating agencies will be described to help practitioners align their programs and policies with an applicable framework.

At the conclusion of this chapter, readers will have understanding of:

- What do the courts and laws define as “cybercrime”?
- What jurisdictions govern cybercrime investigations?
- What cybercrime laws have been produced since 2013?
- What are “best practices” for cybercrime investigations?

Topic in Cybercrime and its Investigation

Figure 1-1 displays topic categories in the “Cybercrime and its Investigation” knowledge domain.

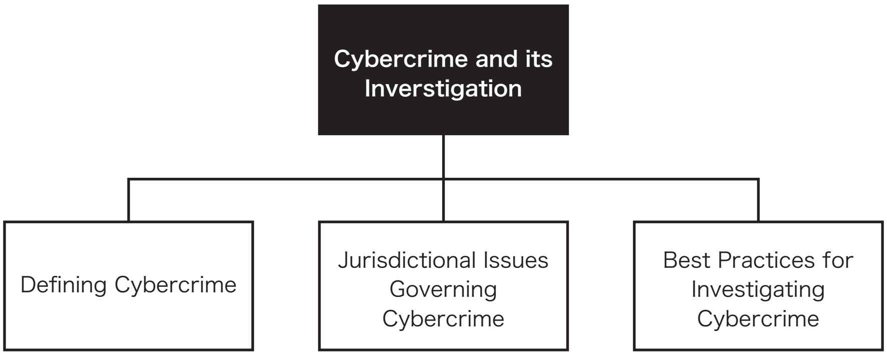

Cybercrime and its Inverstigation
Defining Cybercrime
Jurisdictional Issues Governing Cybercrime
Best Practices for Investigating Cybercrime

Figure 1-1. Topic Categories in the “Cybercrime and its investigation” knowledge domain

Defining Cybercrime

In current (common) definitions there are two broad categories for defining cybercrime[4]: those involving the computer as a tool or instrument of the crime and those involving the computer as a target, or victim, of the crime. In the first category, the computer (or computing technology) is a tool or instrument that enables the perpetrator to carry out criminal activity. For example, a child predator may use a computer to identify, track, and lure young victims that the predator seeks to molest; a thief may use a computer to access bank accounts and misdirect funds; and an unscrupulous competitor may use a computer to steal another' s protected and confidential business information. Conversely, banks often suffer "Distributed Denial of Service" (DDOS) attacks that interrupt their customer services capabilities, impacting their business. This type of attack is reflective of the computer as a target.

An associated third category that has recently emerged is the computer as a distraction or means of distorting evidence to distract investigators from the actual objective(s) of the crime. Although this still represents the use of computers as a tool, in some cases it coincidentally inflicts damage on targeted computers as well. For example, an attacker may gain access to an organization' s computer network with the objective of targeting the financial management system to commit wire transfer fraud, but in the course of their activities they may deploy ransomware to other computers in the network in order to draw investigators and responders away from an analysis of other activities.

Technology as a Tool of the Crime

As we increasingly use computers, mobile computing devices, and automation technology in all aspects of our personal, financial, and business lives, these technologies also are used to commit an ever-growing number of crimes. Today, using a computer is often the most efficient means of accessing the people and information needed to carry out a crime. Also, committing crimes through electronic tools such as online or virtual services can bring perpetrators the added benefits of (1) geographic reach, (2) speed, and (3) anonymity. These benefits for criminals bring greater challenges for victims and law enforcement. For example:

(1) Geographic Reach:

Computers enable perpetrators to commit crimes on a global basis, accessing victims and information worldwide from remote places across the globe. This includes the ability to commit crimes from parts of the world that can be difficult for victims and law enforcement to reach. Consequently, victim companies, law enforcement, and governments must establish international relationships and procedures for investigating and addressing cybercrime that transcend geographic boundaries. There has been considerable progress in this area over the past decade, but there still remains much work to be done to better coordinate and understand different countries' diverse laws and legal frameworks, varying levels of maturity and understanding regarding cybersecurity issues, and unique methods for addressing crimes. This requires,

[4] Many law enforcement agencies around the world define cybercrime in a manner similar to the Royal Canadian Mounted Police- see "Defining Cybercrime from a Law Enforcement Perspective", available at http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada

as discussed in this book, developing thoughtful response plans and efficient and effective international coordination channels to detect, investigate, and prosecute cybercrimes and cybercriminals.

(2) Speed:

Crimes that would traditionally take a significant amount of time now, through the use of computers, can be committed much faster. Indeed, within mere seconds stolen funds can be electronically transferred internationally, enormous amounts of data can be accessed or destroyed, and millions of illegal images of child pornography can be transmitted globally. This rapid pace requires victims and law enforcement to be prepared, nimble, and swift in identifying when and how a cybercrime has occurred and how to respond. Thus, it is essential for cybercrime investigators and the organizations and governments within which they operate to develop and practice an efficient and effective means for investigating a varied array of cyber incidents, and to develop (in advance) a network of public and private sector experts to call upon for assistance as needed.

(3) Anonymity:

In addition to being able to commit crimes, reach victims, and access information from anywhere in the world within seconds or minutes, cybercriminals can use computers in a way that makes it easy to conceal their identity and location. This creates significant challenges for cybercrime investigators seeking to attribute particular criminal conduct to the individuals, organizations, and (possibly) nation-states responsible for that conduct. The means for masking one' s identity and location through computers has developed over the years and created a nonstop challenge whereby law enforcement develops new and improved methods for detecting criminals while criminals adopt new means for evading detection. Moreover, computers can enable cybercriminals to not only mask their identity but also deceive law enforcement by making it appear that others – such as law abiding citizens, other criminals or organized crime groups, or even other governments – are the ones engaging in the criminal activity at hand. Thus, the concept of anonymity is ever-present in cybercrime and requires investigators to: maintain a level of technological sophistication regarding trends and practices among cybercriminals; stay current on the latest methods and means for cybercrime; and investigate criminal activity from a variety of angles, using both technological and traditional investigative measures as appropriate.

Given these benefits to cybercriminals and challenges to law enforcement, it is unsurprising that crimes using computers as a tool are increasing at a rapid rate. For example, the Japan National Police Agency (NPA) reported that "queries about potential online crime cases have gone up nearly 40% in March 2015 from the previous year" and the "financial damage from illegal online bank transfers in 2014 amounted to roughly ¥2.9 billion or U.S. $24 million."[5] The United States Department of Justice reports that "Cybercrime is one of the greatest threats facing our country, and has enormous

[5] Trend Micro's "The Japanese Underground" Report, p. 4 (using exchange rates of US $1 = ¥119.74), available at http://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdf

implications for our national security, economic prosperity, and public safety. The range of threats and the challenges they present for law enforcement expand just as rapidly as technology evolves."[6] One study showed that, in 2015, the average annual cost of cybercrime for surveyed organizations in the United States was U.S. $15 million per year, up from U.S. $12.7 million in 2014.[7] That same study showed that the global cost of cybercrime for organizations in 2015 was U.S. $7.7 million, with the costs greatest for (in order) the United States, Germany, and Japan.[8] Europol recently reported that "cybercrime is becoming more aggressive and confrontational," and the cybercrime problem continues to grow in Europe and worldwide.[9]

Interestingly, a 2024 study[10] mapping the global geography of cybercrime (based on surveyed cybercrime intelligence and investigations experts) found that while many countries house cybercriminals, a relatively small number of countries are home to the vast majority of cybercrime threats (operations and offenders), as measured by a "cybercrime index" denoting the geography of cybercrime in terms of impact (occurrence and impact of crimes plus the professionalism and technical skill of attackers). A handful of countries- including Russia, Ukraine, China, the United States, and Nigeria- account for most of the world' s impactful cybercrime threats. Figure 1-2 below shows countries mapped to the index:

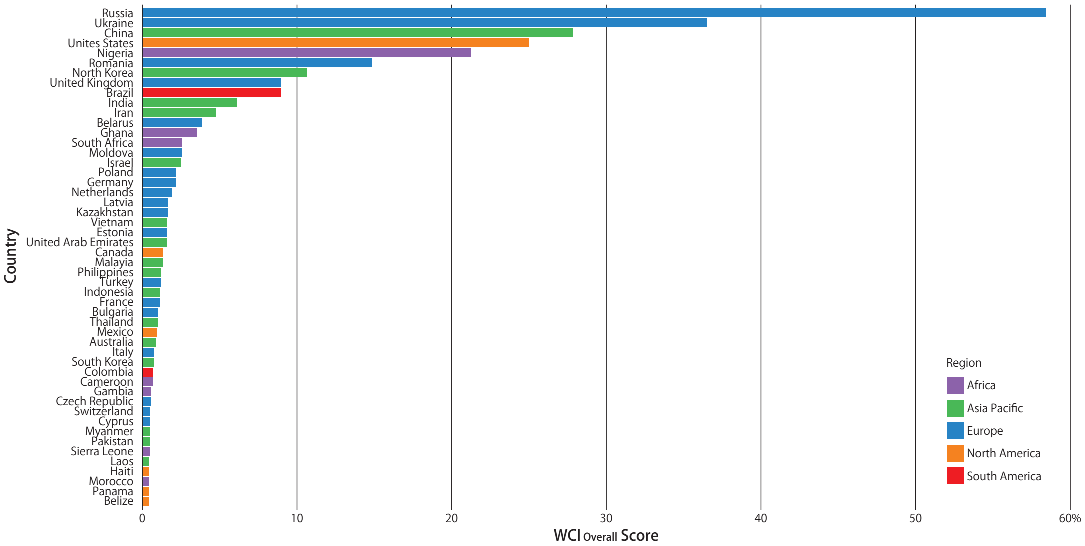


Figure 1-2. Mapping the global geography of cybercrime with the World Cybercrime Index

Cybercrime is deemed more profitable than even the illegal drug trade,[11] and is only expected to

[6] United States Department of Justice website, available at https://www.justice.gov/usao/priority-areas/cyber-crime.

[7] Ponemon Institute, "2015 Cost of Cybercrime Study: United States," October 9, 2015, available at http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states.

[8] Ashley Carman, "Study: Average Cost of Cybercrime Rises Again in 2015 to $7.7 Million," SC Magazine, available at http://www.scmagazine.com/ponemon-and-hp-release-annual-cybercrime-cost-study/article/443433/ (citing Ponemon Institute study).

[9] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2015, by Europol's European Cybercrime Centre (EC3), available at https://www.europol.europa.eu/iocta/2015/overview.html.

[10] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312

[11] See, e.g., Robert Dethlefs, Fortune, May 1, 2015, "How Cyber Attacks Became More Profitable Than the Drug Trade," available at http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/.

continue to expand worldwide as more people use the Internet, including in Japan and elsewhere.[12] This category of cybercrime, where the computer is a tool of the crime, often does not require the perpetrator to possess sophisticated technological skills or knowledge. However, a solid understanding of how to investigate and respond to crimes committed through the use of computers, as discussed in this book, will give law enforcement and corporate victims an advantage in identifying, investigating, and stopping cybercriminals.

Technology as a Target of the Crime

The second category of cybercrime, where the computer or related technology (such as an application service that may be individually hosted or distributed across many computers) is the target or victim of the crime, usually involves a more sophisticated knowledge of technology on the part of both the perpetrators and those investigating the crime. This category involves attacks on computer systems themselves, such as: distributed denial of service attacks that freeze or significantly slow down a system' s operations; network intrusions that infect computers and systems with malware; and other means of damaging, deleting, and altering electronic data and impeding system operations.

As we continue to rely on technology for everything from controlling the temperature in our homes, to medical device functions, to operating critical infrastructure such as national water supplies, power grids, and international flight patterns, the potential scope of crimes attacking computers becomes more dramatic. Moreover, the potential harm from these crimes is now catastrophic. Such crimes can range from individual attacks by a sole actor against a single computer to major threats against a multinational organization or country perpetrated by an organized criminal enterprise or enemy nation-state. Potential harms from these crimes can scale from minor inconveniences and "glitches" impacting individuals and companies, to lost data, to significant threats to public health and safety, to full-scale cyberwarfare.

This area of cybercrime will likely continue to grow exponentially in light of our expanding reliance on computers to efficiently manage all aspects of a country' s infrastructure and a company' s operations. For example, cybercriminals have launched an increasing number of attacks on computer systems using "ransomware," whereby they take systems or electronic data "hostage" and will not restore the owner' s access without a "ransom" or financial payment. In 2015, the United States Federal Bureau of Investigation received 2,453 complaints regarding ransomware attacks which cost victims an estimated US $24 million.[13] Ransomware attacks also are increasing significantly in Japan. According to a Trend Micro report, in 2015, Japanese companies reported 650 cases of ransomware infections, which was more than 16 times the number of ransomware attacks reported in 2014; and in only the first three months of 2016, companies had already reported 740 ransomware cases in Japan, showing the problem continues to grow.[14] The ransomware problem is also prevalent throughout

[12] See, e.g., Tom Reeve, SC Magazine (U.K.), Oct. 15, 2016, "Japan Facing Explosion in Cyber Crime Claims," available at http://www.scmagazineuk.com/japan-facing-explosion-in-cyber-crime-claims-report/article/446174/, discussing Trend Micro's "The Japanese Underground" Report, available at http://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdf

[13] David Fitzpatrick and Drew Griffin, "'Ransomware' Crime Wave Growing," April 4, 2016, CNN, available at http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/.

[14] Shusuke Murai, "Ransomware Making Costly Inroads Into Online Japan," The Japan Times, June 6, 2016, available at http://www.japantimes.co.jp/news/2016/06/06/reference/ransomware-making-costly-inroads-into-online-japan/#.V8mgEztrrww (citing Trend Micro report).

Europe and elsewhere. One study of 500 companies in four countries showed that almost 40 percent of businesses were targeted with ransomware in 2015, and 54 percent of all U.K. companies surveyed were targeted.[15]

We should also continue to expect a growing number of crimes targeting computers as a result of the evolving Internet of Things (IoT), whereby technology is increasingly pervading every facet of our lives through an expanding network of connected devices providing (to varying degrees) autonomous computer functions impacting many daily functions; for example, home climate control and security, automobile functions and features, household appliances, smartphones and other portable devices, health-related devices and equipment, and more.[16] Given the potential scope, damage, and complexity of these crimes, it is essential to have a solid understanding of how to prevent, detect, and prosecute cybercrimes targeted at computer systems.

Technology as a Distraction from the Crime

As previously mentioned, besides the use of technology as a tool or as the target of a crime, technology can also coincidentally be used for both purposes. Some complex crimes may employ "false flags" or distraction techniques to obfuscate evidence or distract investigators. In a more traditional (non-cyber) crime, this would be like criminals setting a fire in a High School to distract responders away from a jewelry store robbery.

When computers are used as a distraction from the crime, the criminal typically first estimates the capabilities of the organization to investigate and respond to simple computer crimes by probing the target environment. Sometimes, they may simply employ coincidental tactics of distraction and targeted attacks without prior probing or reconnaissance. In either case, cybercriminals attempt to masquerade their activities by deploying tools or attacking computers unrelated to targeted objectives such as theft, subversion, or sabotage of the organization' s computer systems and applications. In such cases, the obvious evidence of computer intrusion and manipulation (or destruction) can overshadow the more ephemeral evidence of a misuse of credentials or computers without the use of malware – or the use of tools unrelated to the distraction techniques. In effect, something "shiny" is more often investigated than something less obvious- and criminals take advantage of this. When investigating cybercrimes, it is therefore crucial to examine the motives and goals of the crime and consider all available evidence in an objective manner.

Laws Defining Computer Crimes

In defining, investigating, and prosecuting computer-related criminal activity, it is helpful to consider traditional criminal laws as well as computer-specific laws to determine whether and how these laws might apply to the conduct at hand. This is true in the context of both crimes committed using technology as a tool, as well as crimes where technology is the specific target. For example, laws under a country' s or region' s penal code pertaining to theft, bank fraud, wire fraud, child

[15] Alex Hern, "Ransomware Threat on the Rise as 'Almost 40% of Businesses Attacked," The Guardian, August 3, 2016, available at https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked.

[16] The Internet of Things (IoT) is an evolving network of internet-enabled devices that can communicate with each other and function electronically in a variety of ways impacting daily life. Many devices currently exist and more are being developed in this rapidly expanding area.

exploitation, protection of intellectual property, and other crimes often apply to crimes committed in the computer context. While many of these laws were written long before computers existed, others have been enacted- and some have been amended- to include specific sections that expressly contemplate computer-related violations of those long-standing laws.

Moreover, many nations including Japan and the United States have enacted specific laws governing unauthorized access to computers.[17] For example, in Japan the Unauthorized Computer Access Law-Law 128 of 1999, in effect since 2000- criminalizes unauthorized computer access, providing for up to one year in jail and a fine of up to 500,000 yen.[18] In the United States, the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030, criminalizes unauthorized access to a computer with punishments ranging from up to one year in prison (a misdemeanor offense) to life imprisonment (when intentional computer damage results in death).[19] Other governments including those in the United Kingdom, Germany, Singapore, and elsewhere have also enacted their own versions of computer misuse laws.[20] One challenge in creating computer-specific laws, however, is that both the technology and how people use it rapidly changes. Also, the type and scope of cybercrimes and potential harms from those crimes continue to expand much faster than laws are revised. This makes it important for computer-specific laws to be sufficiently flexible and adaptable so they do not become outdated soon after they are enacted.

●A Diverse Perspective

During a cybercrime investigation, in seeking to define the conduct that has occurred it is most effective to gather evidence with a combination of both a technical computer-based approach- including a forensic analysis of electronic data and information- as well as a more traditional investigative approach that includes interviewing witnesses and reviewing documents, communications, and bank records or other applicable data. Depending on how the evidence unfolds, investigators and prosecutors should keep an open mind regarding the applicable statutes that should be charged. They should consider whether traditional penal laws, computer-crime specific statutes, or a combination of both traditional and computer-specific laws would be most effective and appropriate to charge based on the evidence in the case. In conducting this analysis, prosecutors should also consider the potential applicable penalties, since they can vary greatly based on the laws charged.

For example, a perpetrator may unlawfully access a bank' s computer systems to divert funds

[17] Unauthorized Computer Access Law of Japan, Law 128 of 1999, available at http://www.cybercrimelaw.net/Japan.html and . See, e.g., Takato Natsui, "Cybercrimes in Japan: Recent Cases, Legislative Problems and Perspectives, 2003, available at http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf; Ryan Handerhan, "Japanese and American Computer Crime Policy," 2010, available at http://repository.cmu.edu/cgi/viewcontent.cgi?article=1067&context=hsshonors.

[18] A provisional translation in English of the Unauthorized Computer Access Law of Japan is available at http://www.cyberlawdb.com/gcld/wp-content/uploads/2010/04/computer_access.pdf

[19] The text of the United States Computer Fraud and Abuse Act, Title 18 United States Code, Section 1030, can be found at: https://www.law.cornell.edu/uscode/text/18/1030; a description of that law and related U.S. laws is provided by: Charles Doyle, Congressional Research Service, "Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws, Oct. 15, 2014, available at https://www.fas.org/sgp/crs/misc/RS20830.pdf.

[20] See, .e.g, Clemens Louis, "Comparison of Computer Misuse Acts Around the World," (comparing Computer Misuse Acts of the United Kingdom, Germany and Singapore), available at http://www.rechtsanwalt-louis.de/european_computer_misuse_acts.htm; Michela Menting, "Cybercrime Laws by Country and Other Resources," Oct. 2011, available at http://www.academia.edu/1125166/Cybercrime_Laws_By_Country_and_Other_Resources_DOC.

from the bank and manipulate electronic bank records to conceal the crime. This could fall under a computer-specific law criminalizing unlawful access to a protected computer. The conduct may also fall under laws applicable to theft and fraud. In addition, the potential criminal sentence for the conduct may be greater (and the jury instructions may be simpler) under the equally applicable laws governing bank fraud. Also, depending on the country' s laws, investigators' and prosecutors' definition of the criminal conduct as theft, fraud, unlawful computer intrusion, or all three may change the following: what evidence can be gathered, under what means (such as electronic wiretaps) it can be gathered, the ability to get potentially relevant evidence from other jurisdictions, and what evidence can be introduced at trial. The laws used to charge the criminal conduct may also impact whether (and how) the defendant can be arrested in and extradited from another jurisdiction, as some countries will extradite defendants based on traditional penal crimes but not for less recognized computer-specific crimes.

Moreover, since cybercrime is an emerging area in the courts and relevant technological backgrounds and understandings vary greatly, it is important to describe the crime and the evidence in a clear way that specifically defines what happened, how, and by whom- as it directly applies to the particular criminal laws being charged. This often requires defining technical terms and procedures used to commit the crimes in ways that a judge or juror (whether a professional judge or lay-judge under the Saiban-in system) would understand. Thus, in addition to selecting the most applicable laws to define a cybercrime and charge a defendant, it is also important to sufficiently describe the criminal conduct, computer-specific methods, and means used to commit the crime- in addition to establishing the identity of the defendant as the perpetrator- in a way that people with varying levels of technological sophistication will understand.

Jurisdictional Issues Governing Cybercrime

While cybercrimes can be prosecuted under a country' s general penal laws, computer-specific laws, or a combination of both, complex jurisdictional issues often exist. This is because when it comes to cybercrime, the locations of the perpetrator, the victim, and where the criminal conduct occurred often transcend geographic boundaries. Many countries also have different views on whether, how, and to what extent cybercrimes and related conduct should be regulated. For example, certain activities in one state may constitute a cybercrime while that same conduct in another state may not be a criminal violation. Examples of this include the emerging contexts of cyber bullying, revenge pornography, and intellectual property theft. Moreover, national laws and procedures for collecting, using, and preserving evidence in criminal cases often differ. Another significant problem is that while cybercriminals often act swiftly and electronic evidence can quickly disappear, international investigations are often delayed due to a lack of clarity on what information can be shared through what means and how law enforcement in different countries can best work together.

To determine whether a country or state has jurisdiction over a crime or criminal, there are different potential standards. These include those considering where the offense was committed, the nationality of the offender, the nationality of the victim, the overarching national or international interest impacted by the crime, or where the defendant currently is located.[21] However, even defining "where" the offense was committed can be quite difficult in the cybercrime context. It may be where one or more of the perpetrators were physically located when committing the crime, where the victim or victims were located, where the computer systems or information accessed were located, or all of these potential jurisdictions. Given that cybercrimes can often be committed from across the globe, it is not unusual for more than one jurisdiction to have an interest in the criminal conduct. It also is not unusual for evidence- necessary to determine what occurred and how- to reside in multiple jurisdictions.

As an initial matter, determining the identity and location of the perpetrator can be a significant challenge in cybercrime. A considerable benefit to the Internet is that it creates a measure of anonymity that encourages privacy and unhindered freedom of expression. However, with that anonymity comes a potential risk that criminal actors believe they can act with impunity, particularly given the challenges in determining who those actors are and where they are located.

In the past, a bank robber would be at the physical location of the bank and tangible funds would be transferred from that physical location in a bag; starting the investigation in and around the town where the bank was located made sense. Now, a bank' s computer systems can be accessed from anywhere in the world, funds can be transferred and data can be accessed within seconds, and data can be transferred and resold worldwide within minutes of an intrusion. Addressing cybercrime now requires a far more nimble and sophisticated response by victims, law enforcement, and prosecutors. The sooner a victim or law enforcement can detect and report that an intrusion or other computer crime has occurred and the faster that law enforcement and the victim can work together to determine what was taken and how, the better chance there is of identifying the perpetrator and mitigating the harm from the crime.

Moreover, those investigating cybercrimes in-house and in-government must be aware that criminals often use methods to conceal their location electronically. For example, rather than attacking a bank' s systems directly from the criminal' s computer, the perpetrator may first access (illegally or otherwise) one or more other computer systems and then route the pernicious criminal traffic through those systems to conceal their location. These "hops" through other computer systems can occur in multiple countries, thereby making detection, apprehension, and jurisdictional determinations all the more difficult. In addition, cybercriminals often sit on a computer system for a period of time, infecting it with malware and learning means of access to desired data in order to most effectively obtain information or funds in a way that best conceals the breach entirely and masks what data was taken and how. This creates further challenges for law enforcement responding to an incident since it can take time, effort, and sophisticated knowledge to understand where the true perpetrator may be located and how to fully understand the conduct that occurred.

Due to the complexity of cybercrimes, it is important to understand the complex jurisdictional challenges and international nature of many cybercrimes. It also is important that investigators look for technical clues to best understand what has occurred and where (discussed in Chapter 5), and know how to access available means of international collaboration and information sharing (discussed in Chapter 9) to best respond to a cyber incident, notwithstanding jurisdictional hurdles that exist.

[21] See, e.g., Armando Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime," European Journal of Legal Studies, available at http://www.ejls.eu/6/78UK.htm (discussing different jurisdictional theories).

Convention on Cybercrime

In an effort to find a common international criminal policy to address cybercrime, in 2001 the Council of Europe developed the Convention on Cybercrime, also known as the Budapest Convention, with active participation from Japan, the United States, Canada, and South Africa. The United States and Japan ratified the Convention in 2006 and 2012, respectively, and it was entered into force in the United States in 2007 and in Japan in 2012.[22] As of June 2024, 72 states have ratified the convention and an additional two have signed but not yet ratified it.[23] The Convention specifically focuses on computer-related fraud, copyright infringements, child pornography, hate crimes, and network security violations. Participating countries agree to have domestic laws that criminalize such conduct, including in the cyber context. The Convention also seeks to set a framework for obtaining and preserving computer-related evidence and fostering greater international cooperation to assist in investigating and prosecuting cybercrime.

The Convention was considered groundbreaking and a leading example of countries coming together to seek a more unified solution to addressing the growing cybercrime threat. However, the Convention only goes so far in being effective because countries and victims still need to further develop their own internal processes, positions, laws, and expertise for identifying, investigating, and addressing cybercrime and its damages. There remain many disparate views within and among countries regarding, for example, the scope of privacy protections and how those may impact what measures investigators can take to determine the manner and means of collecting evidence regarding potential crimes using computers. There is also a need for greater education and understanding regarding potential laws that are available to address cybercrime. In addition, the lack of current, relevant, and sufficiently flexible laws that define criminal conduct involving the use of computers as a tool or target of a criminal offense creates challenges in defining and addressing cybercrime across jurisdictions.

MLATs

Another way to address jurisdictional issues impacting international evidence gathering in cybercrime investigations is through Mutual Legal Assistance Treaties (MLATs). MLATs exist between and among a number of countries to enable cross-border cooperation in investigating cybercrime and other offenses. MLATs enable prosecutors to request and obtain information from their counterparts in another country, for use in a criminal matter. One major hurdle, however, is that using MLATS to gather evidence can be time consuming and at times takes years to accomplish. Given the swift nature of cybercrimes and cyber criminals, evidence and perpetrators are often long gone before the bureaucratic steps are taken to obtain information pursuant to an MLAT. There has, however, been a significant improvement between and among certain countries with regard to cybercrime investigations, allowing information to be preserved and shared on a less formal basis as an initial step before the information is more formally provided through the MLAT process.

[22] See Website for Council of Europe, page regarding Convention on Cybercrime, Treaty 185, List of Signatories, available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[23] Id.

Diplomacy

In light of the often complex international issues impacted by cybercrime, understanding diplomatic tools for enabling international responses to cybercrime is also important. As companies become increasingly aware of cyber harms and remedies, more channels of diplomatic discussion and collaboration are being strengthened. A good example of success in this area involves the international response to the 2012 cybercrimes against financial institutions through distributed denial of service attacks. Through international collaboration involving a number of countries, government representatives engaged in diplomatic communications and public and private sectors embraced technical and legal cooperation to help stop the attacks by blocking the Internet nodes, or access points, through which the attacks were conducted.[24]

Regulation

Another jurisdictional issue to consider is that of regulation, both in terms of government regulation and industry or company self-regulation. Given the rapidly evolving nature of cybersecurity, it is not feasible to identify too specific of a framework for proper standards and sufficient security, and laws in many jurisdictions lag behind the problems that need to be addressed in this context. Accordingly, regulators in many jurisdictions have taken a role in overseeing cybersecurity and some industries have embraced industry-specific regulations to help protect the systems and data most vulnerable to criminal attacks. An increasing number of companies also are taking it upon themselves to ensure a greater degree of self-assessment and self-regulation to ensure adequate security for preventing, detecting, responding to, and mitigating harm from a cyber attack. As society becomes increasingly knowledgeable about the importance of proper cybersecurity to protect against cybercriminals, laws and standards will likely continue developing to better define cybercrime and provide additional guidance regarding how best to investigate and prosecute cyber offenses on a national and global scale.

CERTs

In an effort to transcend jurisdictional barriers to improve information sharing and enable law enforcement in different countries to work together, both private sector companies and governments have forged relationships to address cybercrime. These include Computer Emergency Response Team Coordination Centers (CERTs) which exist in Japan, the United States, the EU, and elsewhere around the world.[25] In addition, the FBI has positioned legal attachés in numerous countries worldwide to assist with cybercrimes and facilitate communication and collaboration. Other means for international cooperation also exist, as discussed later in this book.

[24] See, Judith H. Germano, "CyberSecurity Partnerships, A New Era of Public-Private Collaboration," addressing the importance and effectiveness of cybersecurity information sharing and collaboration and effective means for doing so, available at http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

[25] For example, the English-version of the website for the Japan CERT is available at https://www.jpcert.or.jp/english/

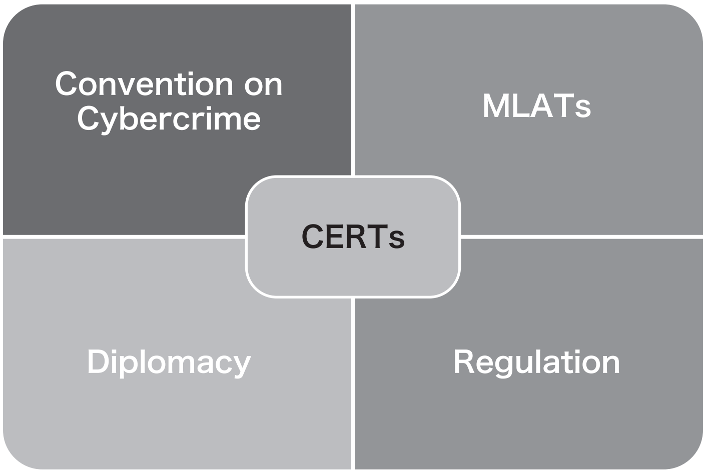


Figure 1-3. Cybercrime Governance

The correlation of cybercrimes' jurisdictional governance is depicted in Figure 1-3. Organizational policies concerning the methods of conducting investigations can be adapted according to related requirements.

Best Practices for Investigating Cybercrime

Determining that a potential cybercrime has occurred may begin with the victim, law enforcement, or a third party. Sometimes an individual or corporate victim may realize that systems are not operating properly, data or funds are missing, or a child has disappeared. Other times, as with the growing trend of cybercrimes committed using "ransomware," a victim may receive a message that a cybercriminal has taken electronic control of a computer or system and will destroy its associated data unless the victim pays a ransom for its release. In other cases, a company' s internal system controls may alert the company that a potential cybercrime has occurred;- this may include technical controls that send electronic reports of suspicious activity on the computer system as well as governance controls, such as an employee knowing and following the process for reporting a stolen laptop containing company information. These are just a few examples of crimes where the victim may first detect the crime and then determine whether (and how) to report the problem to law enforcement.

Other times, law enforcement may receive information about a particular attack against a company or individual who does not yet know the cybercrime has occurred, in which case law enforcement may notify the victim. Law enforcement may receive a tip or have information regarding potential cybercrime trends in industries and reach out to corporate victims. In other cases, law enforcement may determine- based on surveillance or data obtained in another investigation- that a company has been victimized by a cyber attack. One informative source for law enforcement involves covertly monitoring illicit chat rooms and websites used by cybercriminals, including those engaged in crimes against children, credit card fraud, other financial crimes, and other offenses. Another helpful source for law enforcement is other law enforcement agencies in foreign jurisdictions. For example, unrelated investigations in other jurisdictions may have revealed that videos and images of certain children from a particular town or country are being traded on peer-to-peer networks used by pedophiles.

International investigations have also revealed recurring code used to compromise systems or siphon data, in addition to other international trends or information that provide insight to law enforcement.

A third way that cybercrimes are detected is through reports from third parties which provide information or insight into a cybercrime. For example, credit card processing companies may detect fraud connected to a batch of credit cards that were all used at the same victim retailer. Friends or clients may receive suspicious messages purportedly sent by an individual or company but are in fact sent by a cybercriminal who hacked into the victim' s account or systems. Customers may have trouble accessing certain functions of a company' s website or other public-facing aspects of the company' s online system. A news reporter or other source may see or receive a report that illegally obtained data from a particular company is being offered on the Internet' s Dark Web- the electronic version of a black market for illicit transactions and stolen data. A routine third-party forensic audit of a company' s systems may detect that systems have been compromised. An industry-based information sharing group involving private companies or private and public sector entities may reveal pertinent information regarding cybercrimes that have occurred in a particular jurisdiction. Some of these groups are informal loosely-knit associations based on personal contacts while others are more formalized memberships, as described later in this book regarding information sharing (Chapter 9).

These are just a few examples of the many ways cybercrimes are detected. Regardless of how the crime is discovered, it is important to have robust and trusted lines of communication between the private victims, their internal and external technical and legal advisors, and law enforcement investigators and prosecutors. This is necessary to ensure that the criminal activity is detected as early as possible, reported to the proper person or entities, and that the pertinent parties – victims, their technical and professional advisors, and law enforcement- are sufficiently practiced and knowledgeable to take action to prevent, detect, and mitigate harm and stop the perpetrators.

Due to the new and evolving nature of many cybercrimes, many victims and governments still would benefit from a greater understanding of what to do when a cybercrime occurs- that is, when a cybercrime should be reported, to whom and by whom, and what will happen next. This understanding has been improved by governments working to improve education and outreach to potential cybercrime victims. It has also improved due to, on the part of victims, a greater knowledge and appreciation of the types and potential harms from cybercrimes in addition to the benefit of working with law enforcement to address the threat and harms that may have occurred. However, more work still needs to be done in this area.

A Multi-Faceted Approach

To best understand and respond to cybercrime on a local, regional, and global scale, investigators must recognize that the best approach is a multi-faceted and collaborative effort involving the public and private sectors working together. Often, companies within a particular sector (and more generally) can share information with each other to help to limit harm, identify perpetrators, and establish best practices for addressing cybercrimes. This can help build awareness regarding potential methods and means of attack, the best ways to fortify systems, and available defenses to prevent, detect, and respond to cybercrimes. In addition to collaboration between and among companies, there are great benefits in addressing cybercrimes through public-private programs for information sharing and cooperation on both a formalized and informal relationship-based level.

As an important first step, many companies are establishing and bolstering systems of corporate governance which involve an enterprise-wide cybersecurity strategy. This has become essential given the increasing level of cyber attacks and significant harms they can cause, as well as the realization that the government' s ability to prevent and prosecute cybercrimes is to a degree limited. Often, as noted above, it is the victim company who first determines a cybercrime has occurred, as many private companies have greater resources and specific access and insight into their systems which enable them to identify and address cyber threats. That said, the government, for its part, often provides a breadth of understanding regarding potential cyber threats and trends which offers valuable insight in addressing cybercrime. The government also can engage in proactive means for gathering evidence and identifying cybercriminals, including through search and seizure warrants, covert operations, and arrest warrants and prosecutions, none of which are available to private actors. All of these combined perspectives and tools can play an important role in addressing the growing problem of cybercrime.

Internal Protocols

Within companies, it is important to establish clear lines of communication built upon effective collaboration between the company' s internal (and external) experts who have insight into the security and vulnerabilities of computer systems and information, and senior management who are ultimately responsible for managing risk within the enterprise. For many years, the technical aspects of many companies and computer-related vulnerabilities were relegated to information technology functions that did not have access to senior management. In addition, senior management often lacked concern and knowledge regarding the security of company data and computer systems. As cybercrimes and their potential harms have significantly increased, many organizations now appreciate that a strong system of internal corporate governance regarding cybersecurity is not only important but critical to the organization' s health and- potentially- its survival. This recognition and the allocation of human and financial resources to address cybersecurity are increasingly necessary, particularly given the rise in cybercrime and potentially devastating impacts to an organization, its clients, its customers, and the public at large. Accordingly, top decision makers in organizations must ensure that the appropriate senior leaders are properly aware of and responding to cybersecurity risks and responses.

External Resources

In addition to internal communication and governance structures within an organization, it also is necessary to establish external resources and communication channels to assist in detecting and responding to cybercrime. This includes identifying and developing relationships with external forensic and legal experts to assist in periodic audits of company functions, provide regular updates and guidance to ensure senior management is sufficiently aware of cyber threats and trends, and assist (if and as needed) in the event of a breach. It also is important to develop relationships for information sharing and cybercrime response among industry partners, sector-specific organizations, and government resources. These relationships are discussed in-depth in this book' s chapters on Resolution (Chapter 8) and Information Sharing (Chapter 9).[26]

[26] See also, e.g., Judith H. Germano, "CyberSecurity Partnerships, A New Era of Public-Private Collaboration," addressing the importance and effectiveness of cybersecurity information sharing and collaboration and effective means for doing so, available at http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

Chapter 1: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

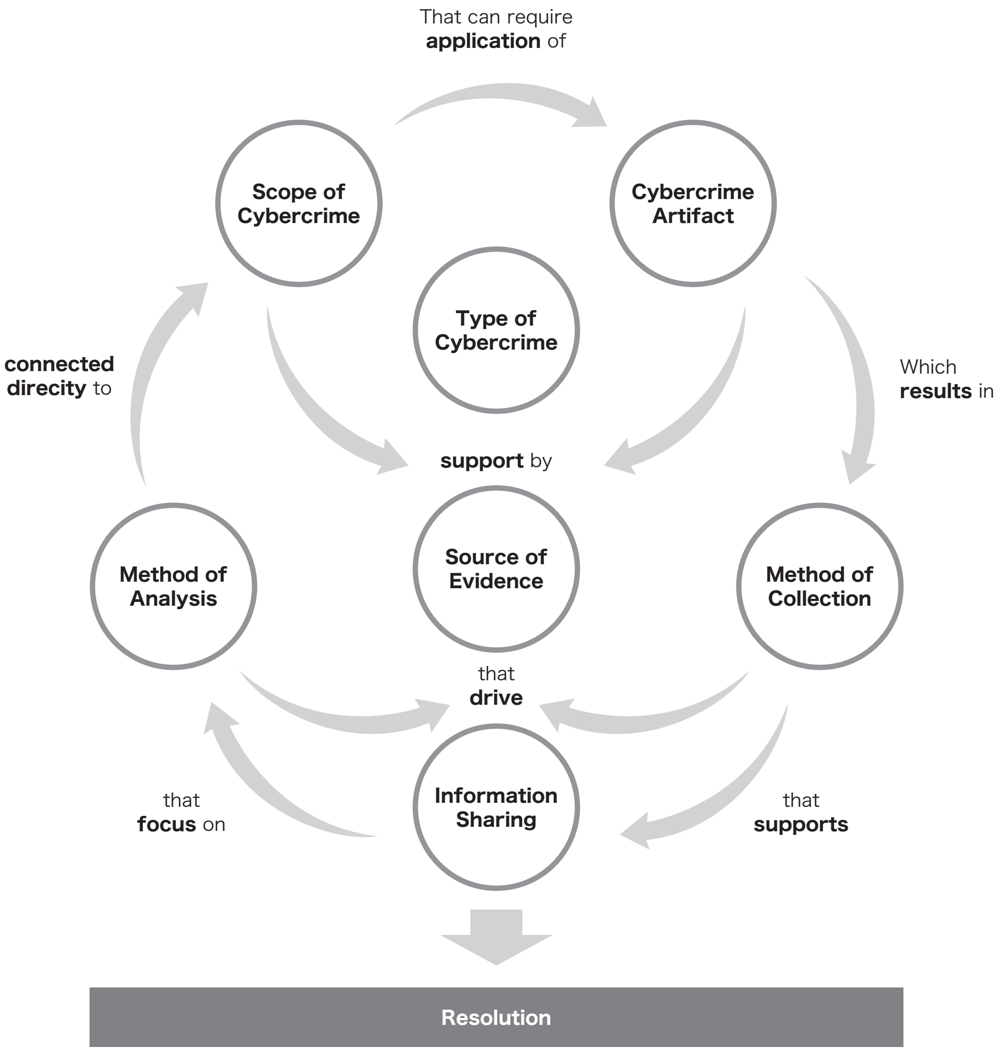


Figure 1-4. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles. The framework includes the activities that are described by the CIBOK. It starts by determining the Type of Cybercrime which details the scope of the crime (for victim impact) and artifacts that illustrate from sources of evidence what the crime was. How evidence is collected and analyzed helps to develop the understanding of the scope of the crime (and type), and the combined sources and collection/analysis methods are useful for sharing information and resolving the incident.

That framework is supported by the taxonomy which describes activities to be performed by the CI function according to required skills, knowledge and experience. Those activities in turn relate to specified roles (executive, intelligence, investigation, judiciary, public relations, support, and administrative) that comprise the CI function of an organization.

In a large organization the roles will be distributed to individuals or teams, in a smaller organization (or a less mature) the roles may be combined as job duties within other roles of the organization (such as CI judiciary being combined into risk management or general counsel job descriptions, or investigation being combined into information security administrator job descriptions or etc.). The roles are defined by their relationship to organizational strategy, tactics, and procedural management activities.

Figure 1-5. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function approves relevant information sharing and oversees the resolution of cybercrime investigation and risk management procedures to help the organization improve its defenses.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. How the investigation proceeds depends upon intelligence collected and analyzed from available sources.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. How the investigation is conducted depends upon the availability and type(s) of evidence.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. The method of investigation performed by related parties depends upon such guidance.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The results of cybercrime investigation provide opportunity for resolving related risks to the victim and similar organizations or individuals.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 1: Review

1. What do the courts and laws define as "cybercrime"?

   Answer: Crimes committed with the use of a computer.

   Examples: Computers as a tool, as a target, as a distraction.

2. What jurisdictions govern cybercrime investigations?

   Answer: International agreements, Negotiated Agreements, National Law.

   Examples: Convention on Cybercrime (Council of Europe, Treaty 185), MLATs, US Computer Fraud & Abuse Act (CFAA),

3. What cybercrime laws have been produced since 2013?

   Answer: A UNCTAD report found that as of 2014, 117 countries had implemented cybercrime laws, with 82 of them being developing and transition countries (Source: https://unctad.org/press-material/global-mapping-cyberlaws-reveals-significant-gaps-despite-progress)

   Examples:

   - *US Cybersecurity Information Sharing Act (CISA): This law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. It was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate on October 27, 2015.*
   - *US Cybersecurity Enhancement Act of 2014: Signed into law on December 18, 2014, this act provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research workforce development and education, and public awareness and preparedness.*
   - *US Federal Exchange Data Breach Notification Act of 2015: This act addresses data breaches and was passed in 2015.*
   - *Nigeria: The Cybercrimes (Prohibition, Prevention, Etc) Act of 2015 was implemented to harmonize law and implement substantive cybercrime laws.*
   - *Qatar: Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law was enacted to address investigatory powers, rules of evidence and procedure, international cooperation, mutual legal assistance, extradition, and service provider obligations in cybercrime matters.*

4. What are "best practices" for cybercrime investigations?

   Answer: Objectively assess the evidence of a "crime" committed with the use of a computer (or computing device). Utilize a multi-faceted approach involving internal protocols and external resources.

   Examples: DDOS vs. Spearphishing (CFAA) vs. Wire Fraud vs. Ransomware; involve organizational response and investigation procedures, jurisdictional guidance, and industry intelligence.

Case Study 1: Dismantling the World's Largest Botnet

- **Crime:** Substantive computer fraud, conspiracy to commit computer fraud, conspiracy to commit wire fraud, conspiracy to commit money laundering
- **Suspect(s):** Access broker (botmaster)
- **Means:** Malware, cybercrime-as-a-service (CaaS; selling access to the botnet' s compromised devices)
- **Motive:** Personal (financial) gain
- **Opportunity:** Poor security awareness/hygiene regarding software and VPN downloads, demand for CaaS access brokers amongst cybercriminals

In May 2024, the U.S. Justice Department announced[27] the dismantling of a botnet known as "911 S5"- believed to be the largest in the world- through a coordinated international law enforcement investigation. The investigative effort led to the disruption of the botnet's infrastructure and the arrest of its alleged administrator ("botmaster"), Chinese national YunHe Wang.

The Justice Department' s indictment revealed that from 2014 to 2022, Wang created and disseminated malware which compromised millions of Windows computers worldwide (associated with over 19 million unique IP addresses, including over 613,000 in the United States) to form the botnet. Wang sold access to the botnet's compromised devices (via proxied IP addresses) to other cybercriminals, collecting around $99 million in profits. These cybercriminals then used their purchased access to commit crimes including numerous cyber attacks, large-scale fraud, child exploitation, harassment, bomb threats, and export violations.

●Malware Distribution and Botnet Management

Wang is alleged to have deployed and spread his malware using various methods, including by embedding it within free VPN services he operated (such as MaskVPN and DewVPN) and by bundling the malware within software offered via pay-per-install services (which often included pirated versions or licenced or copyrighted materials). Once compromised, the infected devices were managed and controlled through a network of around 150 dedicated servers, roughly half of which were leased from U.S. service providers. These servers facilitated application deployment and management, command and control, operation of the 911 S5 service, and access provisions for paying customers (criminals).

●Criminal Activities Enabled by 911 S5

Purchasing access to the botnet's proxied IP addresses allowed criminals to mask their identities (and locations) while committing various offenses. The crimes associated with the botnet' s provided access were wide-ranging and included financial crimes bypassing fraud detection systems to steal billions of dollars from financial institutions and government programs (including via fraudulent unemployment claims), in addition to crimes such as stalking and harassment, identity theft, bomb threats, illegal exports, and child exploitation.

[27] https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation

●Investigation, Arrest, and Botnet Disruption

Law enforcement agencies initially identified 911 S5 while investigating a money laundering and smuggling scheme involving stolen credit cards, which had been enabled by access to the botnet' s compromised IP addresses. After a multi-year international effort by various law enforcement entities, Wang was eventually arrested on criminal charges related to malware deployment, botnet operation, and money laundering. The coordinated effort by law enforcement across the United States, Singapore, Thailand, and Germany led to the seizure of numerous domains tied to 911 S5, in addition to new domains and services linked to an attempt to reconstitute the botnet (called Cloud Router). Over 70 servers and 23 domains were seized and numerous malicious backdoors were closed.

Law enforcement agents additionally seized several of Wang' s residences in addition to assets valued at $30 million, and identified additional forfeitable assets worth $30 million. The U.S. Treasury Department also imposed financial sanctions on Wang and his associates Jingping Liu and Yanni Zheng for their association with the botnet, and on three entities linked to Wang. Wang now faces charges of conspiracy to commit computer fraud, conspiracy to commit wire fraud, conspiracy to commit money laundering, and substantive computer fraud. He faces a maximum sentence of 65 years in prison if convicted of all charges.

The disruption of the 911 S5 botnet is certainly a significant achievement in the fight against global cybercrime. Even more importantly, though, this case demonstrates the collaborative efforts of multiple agencies across the globe, in addition to the broad impacts associated with large-scale cybercrime operations and the evolving tactics cybercriminals employ to mask their identities and accelerate their criminal endeavors. It also highlights the global reach and expansive definition of modern cybercrime.

Chapter 2

Types of Cybercrimes

Introduction

In the past, social outcry and demonstrations against injustices ascribed to businesses was the domain of organized groups with picket signs in front of a building. Today, such social outcry is performed with social media or by defacing business marketing information (such as on websites). An objective of those demonstrations used to be impeding customer access to business products and services, or slowing down workers' ability to perform their jobs. Today, the same objectives are achieved through denial of service attacks or sabotage to wipe systems or make them unusable. Extortion used to be performed with embarrassing information or control over access and services that a business relies upon. Today, it is facilitated by ransomware. Espionage (commercial or government) has always existed but is today facilitated by backdoor Trojans that enable remote access and eavesdropping.

Cybercrime has evolved significantly from 2014 to 2023, becoming more sophisticated, frequent, and impactful. The evolution of cybercrime has been marked by an increase in the variety of attacks, the sophistication of methods used by cybercriminals, and the scale of impact on individuals, businesses, and nations. One of the most significant trends in this period has been the rise of ransomware attacks[28] . Ransomware, which involves encrypting a victim's data and demanding a ransom for its release, has evolved from a tool for financial gain to a weapon of geopolitical significance. The use of ransomware in conflicts between countries, such as in the currently ongoing Ukraine-Russia conflict, underscores the growing trend of cyber warfare.

In addition, phishing continues to be a common cybercrime, with phishing victims making up half of all online crime victims in 2022[29] . Cybercriminals have also evolved their phishing and email impersonation tactics to incorporate new trends, technologies, and tactics, such as cryptocurrency-related attacks[30].

The rise of new technologies such as artificial intelligence has enabled attackers to become more sophisticated in their methods[31]. For example, cybercriminals can use ChatGPT to easily construct attacks, designing the layout of a website and incorporating both credential stealing objects and credential transfer objects.[32] Cybercriminals have also exploited less-protected third party networks to get around security systems.

The impact of cybercrime has also grown exponentially. Financial losses from cybercrime have increased over 570 times since 2001, with cybercrime claiming at least 7,303,267 victims and $36.4 billion in losses over a 22-year period. The global costs of cybercrime are expected to reach $10.5 trillion by 2025, up 15% from $3 trillion in 2015[33].

The COVID-19 pandemic amplified cybercrime with uncertainty around remote working and how to protect data. As a result, cybercrime, which includes everything from theft or embezzlement to

[28] https://heimdalsecurity.com/blog/the-history-of-ransomware/

[29] https://surfshark.com/research/data-breach-impact/statistics

[30] https://www.embroker.com/blog/top-cybersecurity-threats/

[31] https://nordlayer.com/blog/evolution-of-cyber-threats-over-10-years/

[32] Roy, S.S., Naragam, K.V. and Nilizadeh, S. (2023). Generating phishing attacks using chatgpt. arXiv preprint arXiv:2305.05133.

[33] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

data hacking and destruction, increased by 600%[34].

In response to the evolving threat of cybercrime, cybersecurity has become a widespread priority. Governments, businesses, and individuals have had to quickly adapt to new threats and invest in cybersecurity measures to protect their data and systems.

What are the "types" of crime that cyberspace facilitates? This chapter will explore the evolution of cybercrimes: from how cyber tools were used to facilitate business interruption and antagonistic brand attacks to how cyber tools are being used to distract investigators from actual objectives that criminal actors are intent upon achieving (sometimes also with cyber tools). Descriptions of such objectives and supporting motivations, profiles of threat actors and victims, and identifying characteristics of cybercriminals will also be provided. Particular attention will be paid to "human factors" involved in cybercrimes, which play a significant role and influence both the perpetration and prevention of these crimes. Relevant human factors in cybercrimes derive from:

1. **Offenders:** Cybercriminals often exhibit certain psychological traits such as impulsivity, thrill-seeking, and a lack of empathy. These traits can lead to a lack of concern for the consequences of their actions, including the harm they may cause to individuals or businesses. Many cybercriminals also exhibit a high degree of intelligence and creativity, which they use to find vulnerabilities in security systems and develop sophisticated methods of attack[35]. While there is risk involved in cybercrime, cybercriminals circumvent perceived consequences due to motivations including financial gain, personal satisfaction, and ideological reasons. These are often underpinned by behavioral theories in Psychology. For example, the Health Belief Model (HBM), a theoretical model that can be used to guide health promotion and disease prevention programs, can be applied to cybercrimes. Perceived Severity, the second component of the model,is described as "the individual's assessment of the seriousness of the health condition," meaning an individual may make the decision to smoke by assessing the severity of the consequence of smoking. When applied to cybersecurity, this indicates that cybercriminals make an informed decision to attack victims by assessing the severity of the consequences.
2. **Victims:** Human decision-making plays a substantial role in the course of a cybercrime. For example, social engineering is a manipulation technique where cybercriminals exploit human trust to obtain confidential information, enabling further cybercrimes. Using disguised communication such as emails or calls, they trick individuals into revealing passwords or personal details[36]. Behaviors associated with human nature- such as short term memory, fatigue, and forgetfulness- can also contribute to a security incident. For example, a fatigued employee is likely to forget to assess and verify a potential phishing email and may click on ransomware embedded within a phishing email, infecting their machine.
3. **Insider Threats:** Insider threats present a complex and dynamic risk affecting both public and private domains. Insiders are individuals who are part of an organization and who have been granted some level of access to facilities, systems, networks, or people to complete their work[37]. Insider threats may be direct or indirect and can manifest in various ways, including in cyber

[34] https://www.embroker.com/blog/cyber-attack-statistics/

[35] https://www.linkedin.com/pulse/psychology-cybercriminals-understanding-mind-hacker-sharma/

[36] https://terranovasecurity.com/what-is-social-engineering/

[37] https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

acts.

4. **Prevention and Response:** Understanding the psychology of cybercriminals can help individuals and businesses better protect themselves. By recognizing the motivations behind cybercrime, individuals and businesses can take steps to mitigate associated risks. Preventative measures may include monitoring employees and spotting early hacker behavior, a tough challenge for modern companies[38]. Traditional approaches to changing employee behaviors have tended to presuppose that human beings are the weakest link in cybersecurity. However, the Nudge theory of behavioral economics- coined by Richard H. Thaler and Cass R. Sunstein- has shown a promising alternative approach which can be applied in cybersecurity: "soft, paternalistic nudges" can help people make decisions that are in their best interests without limiting their choices.[39] In cybersecurity, nudges may be security notifications, messages, and prompts designed to influence specific security behaviors. They guide people toward the right security decision when it matters most. A nudge could be a prompt at the end of the work day prompting a software update. It could be a reminder to complete the latest security awareness training module. Effective nudges are often personalized. For example, rather than a blanket email addressing the recipient as "Dear employee", an email might begin with "Dear Joe Bloggs". Personalized nudges catch the attention of individuals and make it easier to steer people into the right behaviors.[40]

Human factors are integral to understanding, preventing, and responding to cybercrime. They influence the behaviors of offenders, the vulnerabilities of victims, and the strategies for prevention and response[41].

The definitions provided in this chapter will assist organizational policy developers in determining audit and assessment topics as well as defensive and protective mechanisms by delineating the types of threats that cybercrimes reflect.

This chapter will allow readers to acquire an understanding of the following:

- What is "cybercrime"?
- What are the objectives of and motivations for cybercrimes?
- What are the profiles of cybercriminals?
- How are cybercriminals organized?
- What skills and knowledge do cybercriminals have?
- How has cybercrime evolved since 2014?
- How do human factors relate to cybercrimes?

[38] https://www.wallix.com/blog/the-psychology-of-the-cyber-criminal/

[39] https://blog.thinkcyber.co.uk/introduction-to-nudge-theory-for-security-awareness

[40] https://www.cybsafe.com/blog/security-nudges-behavioral-research/#:~:text=What%20is%20a%20cybersecurity%20nudge,day%2C%20prompting%20a%20software%20update

[41] Leukfeldt, R. and Holt, T, (2021). The Human Factor of Cybercrime (Routledge Studies in Crime and Society) 1st Edition; Routledge Studies in Crime and Society

Topic in Types of Cybercrimes

Figure 2-1 displays topic categories in the “Types of Cybercrimes” knowledge domain.

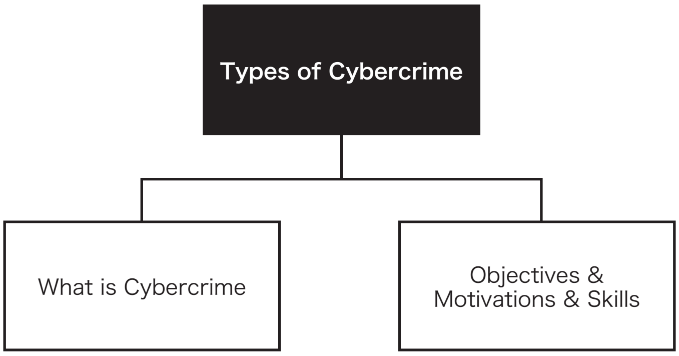


Figure 2-1. Topic Categories in the “Types of Cybercrimes” knowledge domain

What is Cybercrime?

Cybercrime was previously defined as “acts involving cyber space which violate various strongly defined norms in society’ s collective consciousness.” Cybercrime is used broadly to describe a host of criminal and fraudulent actions as well as social activities using the Internet and computers. Society’ s rules of behavior are constantly changing and include common sense courtesies as well as unacceptable behaviors that may or may not be an actual crime.

Chapter 1 provided summary descriptions that can be interpreted broadly:

“Cybercrime[s] ...are crimes committed using a computer (or computing device) as either a tool or a targeted victim, or for purposes of distraction.”

Other definitions may be more detailed and enumerate tools as well as activities involved, such as the following definition from :

”Cybercrime includes any type of illegal scheme that uses one or more components of the Internet (chat rooms, email, message boards, websites, and auctions) to conduct fraudulent transactions or transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Cybercrime also applies to generating spam emails, downloading viruses or spyware to computers, harassing another through the Internet, child pornography, and solicitation of prostitution online. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users.”[42]

As the Internet became more available to everyone, the world wide web opened new avenues for the expansion of business opportunities for many people. Online shopping, email, instant messaging, and other services helped level the playing field for small businesses to compete globally. “Cyberspace” lifted physical limitations for smaller companies who were no longer restricted to local markets. This trend was accelerated by the global COVID-19 pandemic, during which 70% of small firms either accelerated the adoption of digital technologies or raised the degree of digitalization in their operations.[43]

Prior to cyberspace, the majority of criminal activity was conducted mostly in one place at a time. When a Confidence-Man (Con-Man) defrauded a local victim, authorities knew that he was physically present in their jurisdiction when the crime was committed. With cyberspace and new technology, cybercriminals can perpetrate multiple crimes in multiple jurisdictions at the same time.[44]

Many have said, “The good thing about the Internet is that everyone is on it.” Conversely, law enforcement and security professionals would counter with, “The bad thing about the Internet is that everyone is on it!” Criminals found cyberspace to be a new frontier for their activities as well. It opened the door for more efficient and widespread fraud schemes as well as a doorway for sexual

[42] http://definitions.uslegal.com/c/cybercrimes/

[43] Parker, C., Bingley, S. and Burgess, S. (2023). The nature of small business digital responses during crises. Information and Organization, 33(4), p.100487.

[44] Al-Musib, N.S., Al-Serhani, F.M., Humayun, M. and Jhanjhi, N.Z., 2023. Business email compromise (BEC) attacks. Materials Today: Proceedings, 81, pp.497-503.

predators and pedophiles to victimize children in their own homes. Computer hackers can remotely compromise a network, shut down systems, destroy information, and steal proprietary secrets.

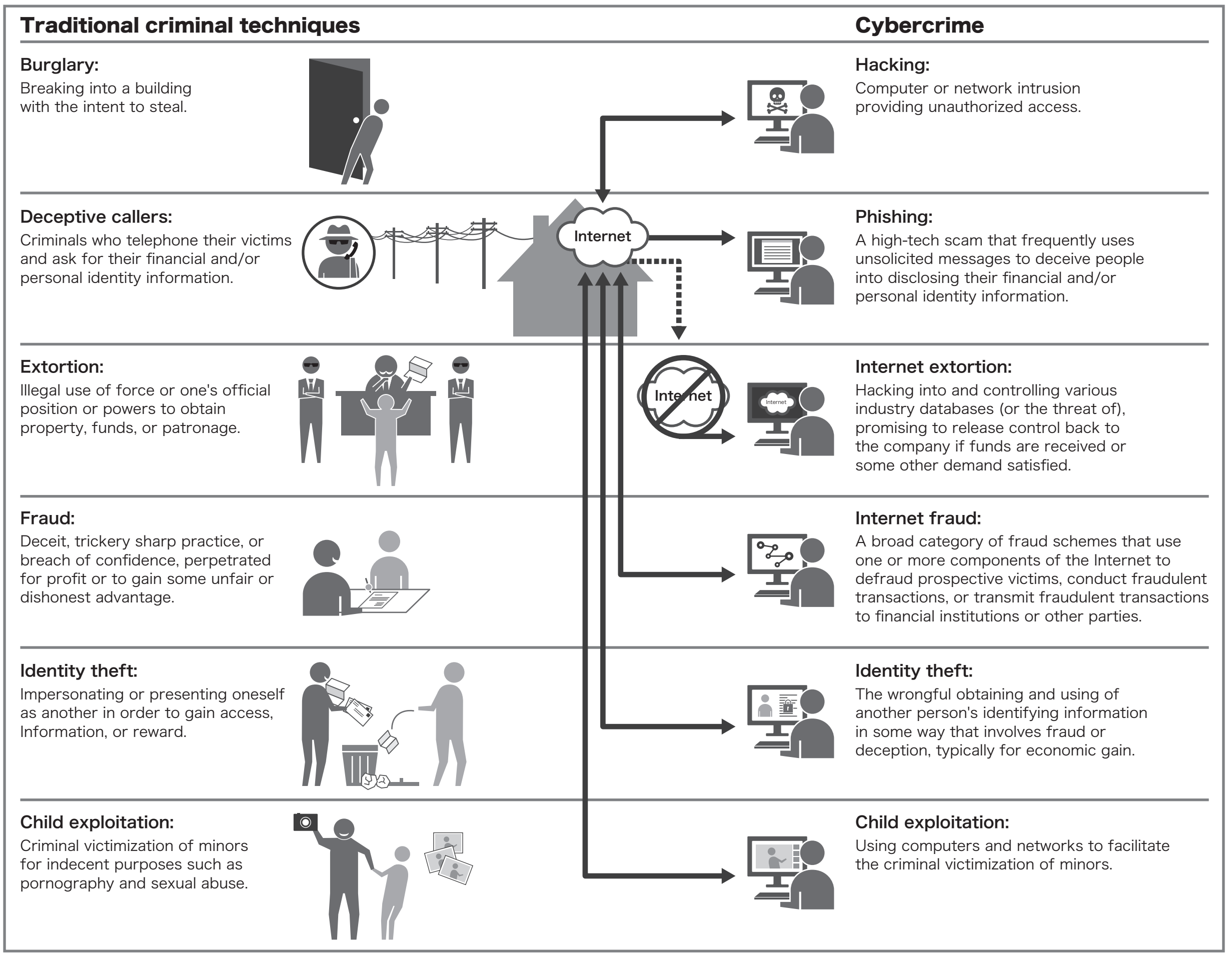
Cybercrime can be literally anywhere cyberspace exists and is at work 24 hours per day and 7 days per week. For example, a cybercriminal can send a phishing email to a large business in the UK while simultaneously sending phishing emails to small businesses and charities in the US, all from a remote location. Automated processes and hosted websites continue to do the work of cybercrime even when criminals are asleep. Malware can lurk on a compromised web page of a legitimate website until an unsuspecting person clicks on a link that makes them a victim. Chat rooms are busy all day and all night, with fraudsters working romance and investment scams alongside pedophiles looking for young people to sexually exploit. Cyberspace has changed the world by globalizing many crimes and creating new ones. For example, cyber criminals capitalized on COVID-19 by exploiting the increased vulnerability and idleness of humans. They increased the sophistication and frequency of phishing, smishing (phishing involving text messages), and vishing (phishing involving voice communication) attacks, aware that individuals were at home without business policies and jurisdictions, and also that businesses were in crisis with little time and few resources to verify the legitimacy of incoming communications.

Cybercriminals take advantage of means, motives, and opportunities which have been made more readily available thanks to the interconnectivity of society[45]. For example, following the COVID-19 pandemic there were reports of scammers impersonating public authorities. Cyber attackers maliciously targeted the World Health Organisation (WHO) and organizations, supermarkets, and airlines[46] by offering COVID-19 cures[47]. These examples demonstrate the widespread vulnerability and cross-sector susceptibility to cyber attacks.

[45] (Pasculli, 2020)

[46] (Threat Team, 2020)

[47] Gervais, J. (2020). Beware Of These Coronavirus Scams. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html> [Accessed 1 September 2020].



Traditional criminal techniques	Cybercrime
Burglary: Breaking into a building with the intent to steal.	**Hacking:** Computer or network intrusion providing unauthorized access.
Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.	**Phishing:** A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.
Extortion: Illegal use of force or one's official position or powers to obtain property, funds, or patronage.	**Internet extortion:** Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud: Deceit, trickery sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.	**Internet fraud:** A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity theft: Impersonating or presenting oneself as another in order to gain access, Information, or reward.	**Identity theft:** The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.
Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.	**Child exploitation:** Using computers and networks to facilitate the criminal victimization of minors.

Figure 2-2. Traditional and Cybercrime counterparts (Source GAO 2007)[48]

Cyber investigators must ultimately identify what crime or activity has been committed and by whom. Examining the victimology, motives, and objectives of cybercrime - and the technical skills required to commit an offense- can narrow the field to identify a perpetrator. Studying victimology can help investigators identify why a person or company was targeted and what the subject' s motive(s) or objective(s) were. The following questions display what an investigator might ask when considering victimology, motives, and objectives: Is the victim on dating and romance websites regularly, or is the victim a contractor that has defense contracts with the government? What type of cyber scam or attack was used against the victim? What skills are required to initiate the crime? Is the perpetrator using chat rooms and social engineering skills, or are they an extremely motivated and highly skilled hacker who can gain access to the victim' s network without detection? Is the victim a teenager or an elderly person? Is the victim targeted for sexual exploitation or because they may have significant retirement funds?

It is important to note that each cybercrime and cybercriminal is governed by different motives and intentions. Fortunately, psychological research provides several theories that help explain behavior and motives, which can in turn be applied to cybercrime. For example, the Health Belief Model (HBM)[49] proposes that perceived vulnerability to disease and disease severity combines to

[48] US GAO, "Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats", GAO-07-705 (2007); source http://www.gao.gov/products/GAO-07-705

[49] Reference: Rosenstock, I.M., 2000. Health Belief Model.

form “threat” and that threat perception motivates action. According to the HBM, threat perception drives behavior but the particular action taken is determined by beliefs about the behavioral options available to counter the threat. A particular behavior will only be adopted if its perceived benefits (i.e., its potential to reduce the disease threat) outweigh its perceived barriers (such as cost, inconvenience, embarrassment, discomfort, etc.). The same theory could be applied to examine cybersecurity behaviors in companies, where cybersecurity policies or behaviors may only be adopted if their perceived benefits (potential to reduce cyber threats) outweigh perceived barriers (cost, inconvenience, etc.).

As discussed in Chapter 1, computers (or computing devices) can be used to commit cybercrimes as a tool (or “instrument”) of the crime, as a target of the crime, or as a distraction from the crime. More generally, the technologies they represent, such as “virtual” services or applications, reflect the same categories when considering the types of cybercrime discussed in this chapter.

Technology as a Tool

The misuse of cyberspace and technology has provided a new tool box for criminals to perpetrate the same fraud schemes and other criminal activities they have committed for years. These new tools allow criminals to become more proficient at reaching a larger victim pool, disguise their activities, and hide their tracks to avoid being caught.

Cybercriminals have also used these tools to manipulate individuals into performing unauthorized or illegitimate tasks. These efforts seek to exploit human psychology and, with correct application, can aid in cybercrime activity.[50] For example, in a 2015 phishing scam, criminals monitored a person in the process of purchasing a home and, after disguising themselves as her solicitor, requested that she transfer £50,000 into their account.[51] A key observation about these attacks is that criminals have sought to exploit many different human psychological traits, including a willingness to trust others, kindness, the impact of anxiety and stress on decision making, personal needs and wants, and the naivety in decision making.[52] In the home purchase example, criminals first targeted the stressful process of purchasing a home and then waited for a specific moment in time where they could impersonate the solicitor to request transfer of funds. The tone of the email emphasized the importance of transferring the funds immediately to secure the purchase. In addition, the home buyer’ s fear of losing the prospective property, the general anxiety of home buying, and the home buyer’ s trust in the (supposed) solicitor are undoubtedly factors that led to the transfer of funds.

Cybercriminals can leverage cyberspace against physical jurisdictions by routing their schemes through other countries in order to avoid detection and make it more difficult for law enforcement to collect evidence. An early example of criminals using technology to their advantage is the use of computer printers rather than typewriters to send written communications to victims. Using an electronic printer not only increased productivity and efficiency in the document preparation process for boiler room fraud operations, but also helped criminals avoid the document being traced back to

[50] Nurse, J.R., 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624.

[51] iTV News: Scammed out of 50,000 over email. http://www.itv.com/goodmorningbritain/news/ scammed-out-of-50000-over-email (2015)

[52] Nurse, J.R., 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624.

the preparer. This adaptation came about when criminals realized that law enforcement laboratory technicians had the ability to identify and match letter keys from typewriters to solve cases involving kidnaping, ransom and extortion demands, and other fraud schemes.

- **Fraud schemes:**

  Fraud schemes have always been based on misrepresentations and trickery. Schemes range from a fake product that is never delivered to a bogus investment opportunity that never materializes. Today, this same trickery and misrepresentation is known as social engineering. Social engineering may be spoken, chatted, emailed, posted or communicated in any manner imaginable. Criminals use trickery during telephone calls, in spam email solicitations for fraud and phishing schemes, and on website postings. Compromised websites can host links that trick victims into clicking on a link and downloading malware onto their computer. Online fraud schemes can be perpetrated against anyone, especially when it is so easy to create an online identity for an individual, business, or organization to create an aura of legitimacy in cyberspace. Today, cybercriminals use phishing emails and social engineering tactics to trick individuals into revealing their cryptocurrency wallet credentials or sending funds to fraudulent addresses. Once obtained, these credentials can be used to steal funds from victims' wallets.

  From a psychological lens, social engineering involves influencing people's decisions in order to accomplish desired results. Its success is at the nexus of psychology and deception, and frequently depends on taking advantage of cognitive biases present in human thought processes. Social engineers know that human reasoning is flawed and manipulate their targets' psychological heuristics into making systematic mistakes to convince them to cooperate.[53]

- **Nigerian fraud schemes[54]:**

  Nigerian (letter or) fraud schemes were initially conducted by sending personal letters via the U.S. Postal Service, placing unsolicited phone calls, and sending faxed communications to intended targets. Technological advances have developed a more robust and cost-effective delivery tool in the form of email. These fraudulent activities range from inheritance and romance scams to national lottery winner scams and investment schemes. Prior to cyberspace, cybercriminals faced investment costs in the form of paper, envelopes, postage, and/or long-distance telephone charges for each attempted scam. Whether their efforts were successful or not, they incurred a cost associated with each attempt on a targeted victim. As technology progressed, cybercriminals began faxing letters, which avoided the costs of sending an actual letter and passed the printing cost to intended victims. Regardless of the tools used in the scam, the utilization of the U.S. Postal Service as a delivery vehicle to perpetrate the scam made it a federal crime as a result of violating the Mail Fraud statute (Title 18 USC §1341)[55]. When criminals moved away from letters and the mail service to the telephone or facsimile devices, their schemes were federally prosecutable under the Fraud by Wire statute (Title 18 USC §1343)[56]. Fraud is still fraud, regardless of how the scheme is delivered or proposed. Both mail

[53] Bosworth, S., Kabay, M. ,& Whyne, E. (2014).Computer security handbook (6thed.). NewYork: Wiley
[54] https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud
[55] https://www.law.cornell.edu/uscode/text/18/1341
[56] https://www.law.cornell.edu/uscode/text/18/1343

fraud and fraud by wire violations were originally investigated as white collar crimes as opposed to computer crimes.

Email has since been embraced by criminals to efficiently deliver spam email scams to thousands of potential victims. Recently, with the use of generative AI, cyber criminals can efficiently create targeted phishing emails using tools like ChatGPT, bypassing alerts and warnings from generative AI tools. For example, a cybercriminal can simply input text requesting ChatGPT to write a phishing email targeted at a CEO of a law firm in the US. While the initial response from ChatGPT may prevent an output and warn the requester, criminals can persist and use simple phrases to manipulate the tool into generating the output. By leveraging generative AI, cybercriminals can easily reduce common errors in phishing email (spelling mistakes, etc.) and make it more difficult to identify scams.

Computer applications allow cybercriminals to prepare elaborate documents using logos and references that give the appearance of legitimacy. Fraudsters also take advantage of crisis situations that are widely reported in the news. Catastrophic events like an earthquake or the "Zika Virus"[57] provide opportunities for criminals to take advantage of others. People are more likely to be duped into donating money to a bogus Disaster Fund[58] or fall for deceptive advertising and purchase a wristband that will protect them from the Zika Virus[59]. Fraudsters also capitalize on international and public holidays like Christmas, as they are aware people are more excited and less guarded than usual and are likely to pursue cheaper purchases. Fraudsters may also conduct "Gift card draining", tampering with gift cards and draining funds before they are used by consumers.[60]

Just like a bank robber researches or cases a bank before robbing it, fraudsters identify potential victims that can be exploited before committing cybercrimes. Criminals use the Internet as an **intelligence tool** to help identify targets. Using Facebook, Instagram, TikTok, and LinkedIn as well as dating websites can aid in identifying potential targets for **romance scams** or **financial grooming (pig butchering)**. Building a persona or profile of targets using these sources can help criminals map introductory statements and pleasantries and in turn build rapport. These methods are social engineering schemes playing on the hope of a non-existent romance or investment in order to separate the victim from his/her money. Romance scams and financial grooming generally share a common thread today. They both exploit emotional vulnerabilities and rely on social engineering tactics to either obtain cryptocurrency wallet information or assets from a victim, or otherwise to lure the victim into volunteering funds to the bad actor under false pretenses and guises leading to the theft of digital assets. These schemes may play out over the course of weeks or months as the bad actor(s) utilizes various social engineering techniques, such as rapport-building and character development, to eventually raise an ask that leads to the transfer of funds/assets.

Internet intelligence efforts can also aid criminals in targeting victims by age. If criminals have a list of names or email addresses, they can simply enter them into a web browser and follow

[57] http://www.cdc.gov/zika/about/

[58] http://www.fraud-magazine.com/article.aspx?id=4294978232

[59] https://www.ftc.gov/news-events/press-releases/2016/05/marketers-mosquito-shield-bands-pay-300000-barred-making

[60] https://www.ftc.gov/news-events/press-releases/2016/05/marketers-mosquito-shield-bands-pay-300000-barred-making

links that provide free background checks to determine the age of a person without subscribing to the service. **Senior citizen scams** target older victims because they are perceived as having a lot of money saved for retirement and more easily socially engineered than young people.

The **Grandparent Scam**[61] is a social engineering scam that exploits the loving, supportive relationship that most grandparents have with their grandchildren. Technology is used as a tool to initially identify a potential target by age and find a telephone number to call. An online money transfer system then used asa tool to deliver money to the fraudster.

This scheme involves tricking the grandparent into sending money to help their grandchild out of a short term financial crisis. The caller starts by calling a phone number of someone who has been identified as potentially having grandchildren (older adults). The caller does not need to know anything more to initiate the scam. Here is an illustration of how a Grandparent Scam might unfold:

Caller: “Hi Grandpa. Do you know who this is?”

Victim: “Yes, this sounds like Matthew.”

Caller: “Yes, it is! So, I was on my way to Canada with a friend and we hitched a ride with a guy in a pickup. The police stopped him for some reason and found that he had marijuana! We all got arrested and I need $500 to get out of jail. I don’ t want mom and dad to find out because that will only make things worse. Can you please help me?”

The victim is then directed to send money using a money transfer system like Western Union.

Table 2-1 outlines the most common scams financial scams targeting seniors:

Table 2-1. The “Top 10 Financial Scams Targeting Seniors” [62]

1	Medicare/health insurance scams
2	Counterfeit prescription drugs
3	Funeral & cemetery scams
4	Fraudulent anti-aging products
5	Telemarketing/phone scams
6	Internet Fraud
7	Investment schemes
8	Homeowner/reverse mortgage scams
9	Sweepstake & lottery scams
10	Grandparent Scam

- **Bullying and Extortion:**

Basic social norms such as saying “please” and “thank you” are taught to young children

[61] http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf

[62] https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

as appropriate responses in certain social situations. Children also learn that bullying is not acceptable behavior. Bullying was originally defined as a **physical intimidation** that occurred where the victim is forced to do something they otherwise would not do. Pushing, hitting, and taking things from the victim were seen as bullying. Bullying occurred when the offender exerted their perceived physical power over the victim to bend them to their will.

Cyberspace is the playground for **cyber bullying** and can extend beyond school to the workplace. Sending text messages, videos, and photographs or spreading untrue stories about someone are all part of cyber bullying. Since social media connects everyone regardless of physical location, the perceived power that a bully holds over another is no longer limited to just physical intimidation. Moreover, cyber bullying can occur at any time day or night, with text messaging and social media postings that can be sent from anywhere anonymously. Bullying, whether in cyberspace or not, can have long term physical and psychological effects on victims. Accordingly, most states have enacted laws concerning cyber bullying and electronic harassment.

Similar to bullying where victims are forced to do something due to threats and intimidation, the misuse of technology has provided tools for criminals to advance their extortion practices. **Extortion** is obtaining something of value, usually money, through force, intimidation, or threats. In the late 1990' s, Microsoft Chairman Bill Gates received a threatening letter to pay $5 million or Gates, his wife, his daughter, and his colleague Steve Ballmer would be killed by a sniper' s bullet. The initial threat was in an extortion letter mailed to Gates from Palatine, Illinois, near Chicago. In order to cloak his identity, the extortionist directed Gates to use a specific Bulletin Board System (BBS) on America Online (AOL) for future communications. Through subsequent letters and postings to the BBS, the FBI determined 800 individuals had accessed the specific BBS during the relevant time frame, with 79 registered in the Chicago area. When the perpetrator sent a floppy disk to use as a new correspondence vehicle, the FBI forensics examiners recovered data that eventually lead to the identification of Adam Pletcher in Palatine, IL, who was subsequently arrested, prosecuted, and sentenced to 70 months in prison[63].

Cyberspace has also provided a new form of extortion that has grown out of **sexting** – sending sexually explicit photos of oneself to others. Criminals befriend females in chat rooms and convince them to send provocative and nude photographs and videos of themselves. When the victim has regrets and refuses to continue to send more, criminals threaten to send the images and videos to their parents, teachers, friends, and church members to force them into compliance. Adult females have been extorted into continuing a sexual relationship with a criminal after being threatened.

Sometimes, after a relationship has gone bad and the couple breaks up, a revengeful partner publishes nonconsensual pornographic photos and videos on the Internet of their former partner. This is referred to as **revenge porn**.

Sexual Exploitation of Children is one of the most prolific criminal behaviors and has grown exponentially with the misuse of technology and cyberspace. Persons involved in child pornography (CP) and the molestation of minors were off of the public' s radar for many years. The public was unaware of the number of people with the proclivity for this activity or the

[63] http://community.seattletimes.nwsource.com/archive/?date=19980711&slug=2760562

number of incidents that occurred. For years, most people did not realize that these offenders were most often not a stranger in a raincoat but rather someone close and trusted by the family and victim. Crimes went unreported for decades. CP photos were usually made with Polaroid cameras because offenders could not risk developing photographs at a film processing store. Videos were even more scarce and were only shared among offenders as brown packages sent through the U.S. Postal Service.

The U.S. Postal Inspection Service was the first federal agency to investigate these types of cases. Like many crimes perpetrated though cyberspace, the Internet expanded the victim pool immensely beyond what used to be a limited physical and geographical area. In the 1990' s, the technology and affordability of digital photography and the ability to trade images anonymously via the Internet exploded into new opportunities for offenders. Due to the availability and anonymity of this type of media and the ability to be connected with like-minded individuals privately online, many pedophiles and molesters came out of the shadows. The advent of **Internet Chatrooms** has also been exploited by these criminals to socially engineer and groom young victims remotely in their own homes. According to the U.S. Postal Inspection Service, one in seven children between the ages of 10 and 17 have been sexually solicited or approached via the Internet[64]. Only 12% reported this to a parent.

Technology as a Target

As criminals became more sophisticated and knowledgeable about using new technology, technology itself became the target and new crimes emerged that did not exist prior to the advent of cyberspace.

- **Card Skimmers:**

  Card Skimmers came about as technology changed the handling of credit cards. Historically, stealing credit card account information was accomplished by "dumpster diving." Criminals would sift through the trash of a business to find carbon slips that were discarded after a credit card was imprinted onto a carbon copy form and signed by the customer. One copy of the slip was given to the customer, one was retained by the store, and one copy was sent to the bank as a deposit item, and the carbon paper between each form was thrown in the trash: there were no magnetic data strips on credit cards at the time. The discarded carbon paper contained the account holder' s name, the account number, and the card expiration date. Armed with this information without anyone being aware of the compromise, the criminal could order merchandise over the telephone and have it shipped to a vacant residence where they would leave a note on the door advising the delivery person where to leave packages if no one was home. There was no trail leading to the offender. The short term fix for this type of "dumpster diving" scam was using carbonless credit card slips.

  As the technology for credit card processing evolved, necessary data was instead stored on a magnetic strip on the back of the card and was captured at the Point-Of-Sale (POS) registers when the seller swiped the card. The data is then sent into cyberspace where it is relayed to the credit card issuer and the vendor' s bank for immediate posting. This process increases security

[64] http://docplayer.net/16377727-A-u-s-postal-inspector-s-guide-to-internet-safety-for-children.html

for account holders as their data is electronically read and transmitted, making it more difficult for criminals to obtain it.

As technology continued to advance, it changed the playing field for criminals. Since they had to obtain physical access to credit cards to steal account information, they needed to target the new card processing technology. Criminals started using their own card readers, or “skimmers”, to capture the information. In a restaurant, for example, a waiter walks away with your card and returns it a few minutes later. This gives ample opportunity for a criminal to skim and capture the card’ s data with a skimmer stored in his pocket or near the cash register. Subsequently, a duplicate card can be made by generating and attaching a magnetic strip to a new plastic card.

Card skimming devices are also placed as false fronts to ATM machines and gas station pumps. When the customer (victim) swipes the card in a skimming device, he/she is unaware that their data has been stolen because it appears that the reader of the device (e.g. ATM or gas pump) simply failed. Moreover, the victim may be alone at an ATM or gas pump and therefore not realize what has happened. The criminal can subsequently remove the skimmer and obtain a collection of data from several credit cards. In 2015, 70% of payment card skimming incidents included in the 2016 Data Breach Investigations Report by Verizon[65] were blamed on criminal organizations.

Before cyberspace, business records such as merger plans, product research and development projects, and corporate communications were difficult to intercept or otherwise obtain. Much like the business of spying, criminals first had to find the business or organization with the data or information sought, find a way to get into the facility and locate the targeted information, and then successfully exfiltrate the data without getting caught. This was even more challenging if the information was stored on an in-house data system.

At one time, spy agencies used a micro camera to take photos of documents. This small device was easy to conceal and transport. 50 exposures for each roll of film would be delivered to the handler or Case Officer covertly at a later date. The landscape of such activities has changed significantly due to the ease and ability to retain and transfer documents electronically. These technologies have opened the door to massive data thefts that previously would not have been physically possible (in most cases).

Approximately 65,000 Word documents or 10,000 PDF documents can be stored on a one (1) gigabyte (GB) thumb drive. A criminal using an 8 gigabyte thumb drive can easily steal 520,000 Word documents and walk out with them or courier them out of a location. Further, using a file transfer program it would take less than 1.5 minutes at 100 Mbps Fast Ethernet to remove 520,000 documents from the location. In contrast, before the advent of USBs this would require a spy to physically remove 104 cases of 8.5” x 11” paper containing 5,000 documents each undetected from the victim site. Insiders today can exfiltrate data using Dropbox™, Google Drive, and other online storage services from their employers or networks they have infiltrated. An important distinction to keep in mind when discussing stolen digital information (whether it is an insider or external threat) is that criminals steal electronic copies rather than original records, making it difficult to detect and prove theft since stolen records are still present in their original location.

In the early years of computer crime investigations, Eastern European hackers would initiate

[65] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

a **computer intrusion** followed by an **extortion demand**. Cybercriminals would gain unauthorized access into a company' s network, steal sensitive information, and then send an email with a veiled threat stating words to the effect of "*We are a consulting security company from the Ukraine and have conducted a free security scan of your system. We have found vulnerabilities which we can fix for a price. To illustrate our authenticity, we' ve attached information from your system to validate our claims that your system is subject to being compromised.*" They would include attachments like a sensitive email from the CEO' s account or a list of accounts and passwords, or anything that would prove that the hackers had access to the victim' s internal network. The message would continue with a veiled threat such as, "*You do not have to hire us, however, we cannot guarantee that someone else will not find these security holes and use them for other purposes.*" In other words the criminals were saying "Pay us or suffer the consequences".

- Insider Extortion Threats:

Insider Extortion Threats are on the rise, according to security firms. Cyberspace has empowered employees to launch public affairs campaigns against their former employers. Ransom payments have even been made to remove a website that was created by a dismissed and disgruntled employee. Approximately 200 people joined the website to post disparaging comments about the company and its management. Some of the comments contained confidential information while others were made up and untrue.

Internal data theft by a disgruntled or departing employee is also a cybercrime risk to an organization or company. Employees may steal intellectual property information to take with them as they begin a job with a new employer. Disgruntled employees may seek revenge or retaliation by leaking information publicly to embarrass the company or damage systems used in product manufacturing, causing physical injuries to current employees.

- Malware:

Malware is a term used to describe malicious software and includes viruses, Trojans, worms, spyware, and ransomware. Malware is used to infect computer systems and automatically execute a routine (or routines). For example, malware might install a backdoor and allow remote access to a victim' s computer as well as collect usernames and passwords and send the information to the attacker. Other malware may set up distribution systems on the victim computer in order to host child pornography images and copyright protected materials such as computer software, music, and videos. Malware can also install a **rootkit**, software that modifies the operating system of a victim computer and replaces key functions with its own functionality in order to maintain a stealthy presence and remain undetected. Malware is also used to take control over victim computers so they can be used as zombie computers to send email spam or as agents in Distributed Denial-Of-Service (DDoS) attacks.

Malware can be delivered in an email as an executable program or as a link to a website that hosts the malware. The attacker must socially engineer the recipient into opening the attachment or clicking on a link. Anti-virus software can block executable programs that are sent as email attachments. However a link to a webpage that may contain malware opens another door to a computer, as the code comes in through a web browser rather than an email system. Email attachments can be any type of file such as a PDF or Microsoft Word document. The executable program is hidden inside of the document file. Microsoft Word documents may contain hidden code in the form of a macro. When the recipient enables macros in Word, the malware executes. Many times, malware is disguised as a security program that allegedly removes malware when in truth it actually installs it. Mcan execute almost any action an attacker needs it to.

Ransomware and Scareware are two types of malicious code that have been widely used for economic gain. **Ransomware** is malware that encrypts the victim machine' s data and renders the data inaccessible. The criminal demands an extortion payment before providing an encryption key or code which will restore the data to a useable state. Ransomware is usually delivered in Trojan attachments such as "CryptoLocker"[66] in an email message. These activities have become highly automated, with criminals distributing malware using a Botnet and hosting the key to unencrypt the victim' s data on a remote server with a timer set to automatically erase the key if payment is not made within a specified time. Ransom payments can be made using Bitcoin or other digital currency, and victims pay amounts ranging from $100-300 for individuals to thousands of dollars for other entities. The market is evolving for malware which has previously been a one-on-one business. Today, developers are selling Ransomware as a Service (RaaS) and distributing malware at no charge to criminals while retaining 40-50% of each ransom payment received. According to a 2016 research study[67], the average Russian ransomware boss makes $90,000 a year. Costs to victims add up. In 2015, the FBI' s Internet Crime Complaint Center (IC3) received notifications from 2,453 victims who suffered financial losses from ransomware schemes totaling $1,620,814[68].

Scareware is malicious code used to socially engineer a victim into purchasing unnecessary software such as anti-virus protection based on a false representation. Operation Trident Tribunal was a 2012 law enforcement task force that targeted an international cybercrime ring that distributed scareware to approximately 960,000 victims who lost more than $71 million purchasing fake security software[69]. The scheme tricked consumers into infecting their own computers with malicious scareware. The scareware presented pop-up warnings that victim computers were infected with a host of malware and forced victims to purchase fake antivirus software to fix a non-existent problem. This case involved the FBI and law enforcement entities in Ukraine, Germany, Netherlands, Great Britain, Latvia, Canada, Romania, Cyprus, Denmark, and Austria.

- **Denial of Service (DoS) Attack:**

Denial of Service (DoS) is an attack method used to overwhelm the services of the victim. Attackers flood targeted machines or networks with junk data requests which overwhelm them (similar to trying to drink from a fire hose). With too many data requests eating up resources, legitimate users are denied service. A Distributed Denial of Service (DDoS) attack involves thousands or millions of machines from different IP addresses that flood the targeted system(s) with continuous data requests, denying service for legitimate users or customers. DDoS attacks can involve millions of zombie machines that have been infected and stand by for instructions

[66] http://www.trendmicro.com/vinfo/us/security/definition/ransomware
[67] https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf
[68] https://pdf.ic3.gov/2015_IC3Report.pdf
[69] https://www.justice.gov/opa/pr/payment-processor-scareware-cybercrime-ring-sentenced-48-months-prison

from a Command and Control machine to identify the time of attack and target IP address.

Hacktivists are cyber activists. They take direct electronic action against social change or perceived injustices by shutting down websites with DDoS attacks. One of the most well-known hacktivist groups is known as "**Anonymous**". Anonymous has been credited with several high profile DDoS attacks against government, corporate, and religious websites. Operation Avenge Assange was an Anonymous coordinated DDoS attack on several financial and credit card companies in protest of the effort to silence WikiLeaks from publishing secret U.S. diplomatic communications in late 2010. Julian Assange is the founder and publisher of WikiLeaks, a publisher of leaked documents and communications. Under legal threats by the U.S. Government, Amazon.com removed WikiLeaks from its servers and MasterCard, Visa, and PayPal cut off services to WikiLeaks. In protest, Anonymous launched DDoS attacks against MasterCard, Visa, and PayPal's main site, which was brought down for a short time causing an estimated $5.5 million in losses to the company.[70]

- **Identity Theft:**

Identity Theft refers to the use of another person's Personal Identifying Information (PII) for economic gain. PII refers to a person's name, date of birth, and Social Security Account Number. Identity Theft alone is not considered a crime by the FBI- the crime is determined by what the thief does with the information. When PII is used to open or access a bank account, apply for credit cards or a mortgage, or purchase property or vehicles, the actual crime and benefit to the perpetrator occurs. The Federal Trade Commission (FTC) reported it received around 1.4 million reports of identity theft events in 2020—twice as many as it did in 2019. There were roughly 394,280 instances of identity theft used for unemployment insurance benefits, as opposed to 12,900 incidents recorded in 2019.[71] In some cases, PII data is obtained through a computer intrusion where criminals obtain PII for thousands or millions of people. In such cases, the intrusion or authorized access is a crime as is the subsequent use of the PII.

- **Terrorism:**

The FBI defines **terrorism (according to US 28 C.F.R. Section 0.85)**[72] **as** "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Terrorists utilize the Internet and technology to leverage worldwide connectivity and gain support for their causes and operations. They use technology to spread propaganda and recruit new members. They can radicalize recruits to commit violence based on their ideology and use cyberspace to financing their operations through websites selling products, donations from supporters, money transfer systems, and charities. Technology provides a worldwide audience and recruitment pool as well as secure communications for planning and executing their activities.

[70] https://nakedsecurity.sophos.com/2013/01/27/not-so-anonymous-anonymouses-head-off-to-prison-over-paypal-ddos/

[71] https://www.cpomagazine.com/cyber-security/identity-theft-doubled-during-the-pandemic-as-fraudsters-targeted-covid-19-relief-payments/

[72] https://www.law.cornell.edu/cfr/text/28/0.85

- **Computer intrusions:**

  Computer intrusions can be viewed as high-tech electronic burglary where technology is used as a tool as well as a target to obtain something of value stored on a system. The common term to describe this type of intruder is Hacker. A hacker is someone who exploits vulnerabilities and weaknesses to defeat security technology and gain access to the network. Victims of hackers include everyone from financial institutions, governments, health care facilities, Facebook, Target, Home Depot, the Democratic National Committee, and even the 2016 U.S. presidential candidate Hillary Clinton.

- **Advanced Persistent Threat:**

  Advanced Persistent Threat (APT) activities involve an attack on a victim' s network to gain unauthorized access and retain that access and remain undetected for a long period of time. APT attacks are most commonly associated with foreign government-sponsored hacker groups but may also represent social extremist or organized criminal groups. These groups are trained, well-funded, and have sufficient resources including staff and infrastructure. Many consider the APT Teams to be the "varsity squad" of hackers. They use a variety of techniques to gain access.

  APT actors often use **Spear Phishing** through email messages with attachments containing malicious code or links to hostile websites that are compromised by the team, all of which give them initial access to the network. Once inside, they look for vulnerabilities to expand their foothold. They download tools and malware that can be used to capture additional accounts on services like email servers. Since email clients like Outlook check with the server continuously, hackers can acquire hundreds of accounts and passwords in a few minutes. At this point, they remove their malware and exfiltrate the new accounts for future use. They then start shopping around for data. Email accounts are a good source for information on projects and development, personnel, and liaison contacts as many users store important information in their email. They will also search for other storage sites and start collecting information to steal. Countries such as China are interested in defense information as well as business and vendor information. Realistically, any intelligence that will inform their country can be a huge advantage for business negotiations with foreign companies.

- **Money Laundering:**

  Money Laundering activities today often involve cybercriminals using cryptocurrencies to launder money obtained from illegal activities. By converting illicit funds into cryptocurrencies and then back into fiat currency through various exchanges and transactions, mixing, tumbling, and other on-chain obfuscation techniques, criminals can obscure the origin of funds and ultimately place them back within the financial system for additional placement and layering techniques.

- **Cryptocurrency Scams and Frauds:**

  The rise of initial coin offerings (ICOs) and cryptocurrency investment schemes has provided opportunities for scammers to defraud investors. Ponzi schemes, fake ICOs, and pump-and-dump schemes have all exploited the hype surrounding cryptocurrencies to deceive unsuspecting individuals.

- **Crypto-jacking:**

  Crypto-jacking involves hijacking the processing power of unsuspecting users' computers or devices to mine cryptocurrencies without their consent. Cybercriminals distribute malware or exploit vulnerabilities to install mining software on victims' devices, resulting in increased electricity bills and reduced device performance.

- **SIM Swapping:**

  SIM swapping attacks typically involve the compromise of centralized cryptocurrency exchange accounts, whereby bad actors essentially swap SIM information. This might be the swapping a mobile phone number to a phone utilized by bad actors to receive newly inbound mobile text messages and calls. This swapping allows threat actors to intercept SMS-based two-factor authentication (2FA) codes. In many cases, if a victim has similar SMS-based two-factor authentication set up for their personal email account bad actors can gain access to their email accounts as well, which in turn can provide illicit access to a victim' s cryptocurrency exchange account. At that point, crypto funds are exfiltrated to the hacker' s crypto wallets (or another related repository).

Technology as a Distraction

DDoS attacks have also been used to distract cybersecurity and incident response personnel from the real attack being launched by the attacker. DDoS attacks were designed to overwhelm and cause a machine or network to be unavailable for legitimate purposes, as described above. However, other DDoS attacks are throttled back to appear that they are the attack vector when they are actually just a ploy to hide other nefarious activity. A DDoS attack will often consume website and security teams' efforts while attackers sneak in and drop malware to maintain access or exfiltrate data. A survey released in 2015 by *Neustar*[73] reported that DDoS attacks were becoming smaller and more frequent, and that victims discovered planted malware and data loss after the attacks.

Ransomware sometimes takes the place of DDOS to either interrupt a business or to simply distract responders away from objective crimes as discussed in Chapter 1. For example, in 2016 a hacker group claimed[74] they were hired by a competitor of a Fortune 500 company to plant ransomware and interrupt the release of a product to the market.

In many cases, adware, scareware, ransomware, and even complex backdoor Trojan malware with obvious "Indicators of Compromise" that cause alarms in corporate information security monitoring and detection software and network tools are used while coincidentally other less evident tools (often network administrative tools that already exist) provide access and functionality that cyber criminals need to achieve their objectives. The use of technology as a distraction is a growing trend and creates added complexity in the process of investigating cybercrimes and isolating objectives to understand the motivations and profiles of criminals, and the related scope and impact to victims.

[73] https://www.neustar.biz/resources/whitepapers/ddos-attacks-protection-report-us-2015

[74] http://motherboard.vice.com/read/ransomware-gang-claims-fortune-500-company-hired-them-to-hack-the-competition

Objectives and Motivations and Skills

Profiles of cyber criminals vary based on their motives, objectives, and skills. This is a new area for behavioral science experts, and in fact, profiling serial killers launched behavioral studies into the public eye. In those studies, profiles for violent offenders might give an age range of 30-40 years old. Depending on the victim, the race may be speculated to be the same as the victim' s. The crime scene, whether organized or disorganized, may indicate an education level or type of work an offender may be employed in.

From a cyber perspective, motivations can range from "Script Kiddies" trying to be hackers to pedophile males in their 40' s, to disgruntled employees, to foreign organized criminal gangs, to government--sponsored professional hacker teams. Cybercriminal ages can vary, as some hackers are 13 years old and others are in their 50' s. Disgruntled employees can be any age when they steal data to use for their next employer. Language in communications may indicate that a criminal is from a foreign country and is using a translation program. Money, revenge, sex, secrets, blackmail, extortion, bullying, activism, spying, and bragging rights can all serve as motives for cybercriminals.

Cyber fraudsters

Cyber fraudsters that use technology as a tool to continue their fraud schemes are motivated by economic gain. Their objective is to trick a victim out of money. They are socially adaptive and adept in social engineering and manipulation techniques. They are less skilled in technology but can effectively use it to accomplish their schemes. They can be organized and work as a team like the Nigerian crime rings (who are not necessarily located in Nigeria). In December 2014, the police discovered a Nigerian crime ring consisting of more than 100 members who were running romance and sweepstakes scams in a suburb of Atlanta, GA[75].

Cyber Bullies

Cyber Bullies can be motivated by revenge, boredom, jealousy, peer pressure, feelings of superiority, anonymity, or a desire to not be a victim. These offenders are not high-tech computer experts but can be knowledgeable about apps that can be used to send disappearing messages that leave no record. These bully groups are informally organized with no permanent hierarchy.

Hacktivists

Hacktivists are motivated by a political agenda. They value working on social change, using technology to spread awareness on issues involving free speech, human rights, or freedom of information. Hacktivists tend to be organized, albeit not always with a structured hierarchy as in the Anonymous group. They tend to come from a hacker background and are skilled in gaining access and releasing information to support their cause. Anonymous, for example, purportedly made a DoSer downloadable program[76] available for others to join in DDoS attacks against its targets. In this manner, like-minded persons lacking in computer skills could join in the DDoS attack to take part in

[75] http://www.cbs46.com/story/25551165/police-international-nigerian-crime-ring-operates-out-of-atlanta-suburbs

[76] http://anonhacktivism.blogspot.com/2013/06/dos-tools-2.html

the protest.

Sexual Exploitation of Children offenders

Sexual Exploitation of Children offenders are motivated by sexual gratification. Pedophiles have a sexual preference for children, and some never act on it. Other offenders may not be pedophiles and therefore have no sexual attraction to children, but target children (online and in person) because they are easier and sometimes convenient prey. Some of these offenders are very skilled and organized while others are not. Some go to great lengths to maintain their anonymity online and are careful with who they trade media with, using encrypted channels for communications and data transfers. Others are loners and find like-minded people online who will share their knowledge on what software to use and where to obtain or trade digital media without detection. These offenders are often careful, as federal penalties for their crimes are severe.

Terrorism

Terrorism is defined as threats or violent acts against people or property to affect government policy or political, religious, or ideological change. **Terrorist groups** are sophisticated, well organized, and technically savvy. They know that governments are spending significant resources and using highly trained technicians to track them through cyberspace and thwart their recruiting and radicalization programs, as well as their operational planning and communications efforts. Their motives and objectives are to spread propaganda and radicalize people who are willing to adopt extremist religious or political ideologies that are hostile towards certain societies and values. They also seek to recruit people to join them in their fight overseas or become a home grown terrorist. Profile Analyses show these violent extremists are very diverse and do not fit into standard subject profiles. However, most agree there are three components of the prevailing radicalization model required to join a terrorist group: Grievance, Ideology/Narrative, and Mobilization. Cyberspace aids terrorist recruiters by facilitating worldwide propaganda on their grievances – such as the persecution of a certain group (or ethnicity)- and their ideology/narrative. Mobilization is the third component facilitated by cyberspace, as extremists can interact online with like-minded people and be motivated to take action and execute violent acts.

Computer hackers

Computer hackers who break into systems to test their skills and figure out how security programs work are referred to as ethical or **White-Hat hackers.** These are professionals who are organized and have been authorized by the organization to compromise their network. Their objective is not to steal or destroy data or systems, but to view the activity as a penetration testing engagement. Afterwards, they report any security issues to the organization and make recommendations on how to fix them.

Black-Hat hackers are hackers that gain unauthorized access in order to steal credit card numbers or Personal Identifiable Information (PII) for identity theft. These are the real computer criminals. Their objective and motivation is personal gain, financial or otherwise, and to raise havoc in some cases. They use DDoS attacks against businesses or entities they do not like and are very skilled in hacking techniques and getting past security systems in networks.

Gray-Hat hackers are the middle ground between White-Hat and Black-Hat hackers. These hackers are computer experts who may hack into a system without the knowledge or consent of the owner but lack the malicious or evil intention of a Black-Hat hacker. They may report security issues that they find to a public forum as opposed to the site owner directly.

"Script Kiddies" learn about hacking on the Internet and execute existing scripts or code that is written by others because they lack the skills to write their own. They copy code and execute it without a full understanding how it actually works and what it does. At times, they may not even realize what system they are attacking since they are not necessarily targeting a specific organization but rather an IP address. Script Kiddies tend to be loners and less organized, and can cause damage to systems without intending to or realizing it. These individuals are primarily motivated by self-promotion to gain attention among their peers. They may share information and/or scripts they have obtained via Internet Relay Chats (IRC) with peers.

APT Teams

APT refers to "Advanced Persistent Threat" activities conducted by cybercriminals with defined goals and objectives. **APT Teams** can be the most sophisticated and dedicated hacker groups. Highly trained and well-funded, their objectives are dictated by their task masters who may be organized cybercrime groups, competitive market interests, and/or national government organizations (and sometimes, there are not clearly defined differences between these groups). They are tasked to obtain non-public/protected information such as defense weaponry plans, competitive medical research, logistical supply-chain information, or "insider information" that allows trading ahead of markets. Any intelligence they garner will be of value to their organization or task master. For example, APT teams may collect company data on a target' s employees and products, business plans, vendor relationships, and financial/securities performance before a negotiation meeting between their country officials and the company wishing to do business with them. These types of information provide them with a significant advantage like knowing where the target company' s weaknesses are, and their organization can subsequently devise ways to exploit those weaknesses for their own advantage.

Chapter 2: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the types of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

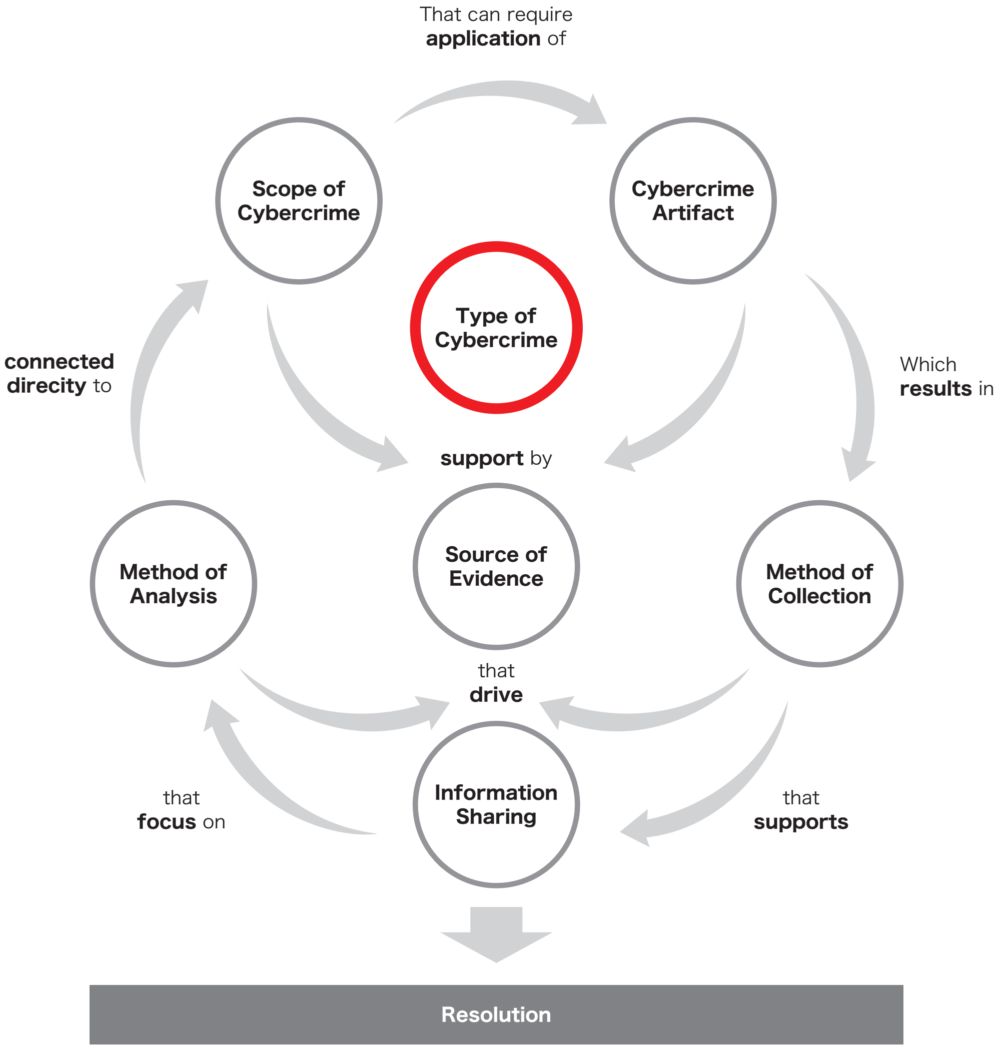


Figure 2-3. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 2-4. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 2-5. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a tactical understanding of associated motivations of cyber criminals and their intended objectives according to how they are organized.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. The type(s) of cybercrime will be determined by evidence.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well as information sharing according to the type of cybercrime committed.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The type of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 2: Review

1. What is “cybercrime”?

   Answer: Crimes committed with the use of a computer.

   Examples: Computers as a tool, as a target, or as a distraction.

2. What are criminal objectives and motivations?

   Answer: Competitive or personal interests to disrupt or harm individuals or organizations.

   Examples: Subversion, sabotage, theft/fraud, espionage.

3. What are the profiles of cybercriminals?

   Answer: Criminals with the technical ability to hire or utilize a computer or related service to achieve their objectives.

   Examples: Anti-societal, extortionist, destructive, anarchist, thief, spy.

4. How are cybercriminals organized?

   Answer: Individually or as a group with similar motivations or direction to achieve an objective.

   Examples: Hackers, service providers, service subscribers, perpetrators of objective crimes.

5. What skills and knowledge do cybercriminals have?

   Answer: Technical and procedural knowledge of targeted systems, processes, or people.

   Examples: Script-kiddies, hackers for hire, APT actors, rogue traders/tellers/employees.

6. How has cybercrime evolved since 2014?

   Answer: More sophisticated, frequent, and impactful.

   Examples: Target of choice or convenience, botnet as a service, dark web services, ransomware increased by 600%.

7. How do human factors relate to cybercrimes?

   Answer: They influence both the perpetration and prevention of cybercrimes.

   Examples: Victimology, Perpetrator Objectives, Outcomes, and Incident Response.

Case Study 2: The “ABC’s” of Cybercrime

- **Crime:** Payment fraud
- **Suspect(s):** IT administrator
- **Means:** Misuse of authorized access
- **Motive:** Personal gain
- **Opportunity:** Inadequate financial systems controls

For a cybercriminal act to be prosecutable as a crime, it has to violate a law. This is one of the biggest obstacles to holding cybercriminals responsible for their actions. To explain this issue, the ABC’ s of cybersecurity must first be understood:

- (A)ttack: Attacks are attempts to get access to a victim’ s network, systems, or devices. Attacks are representative of a physical crime like the attempt to break and enter.
- (B)reach: Breaches are the exploitation of weaknesses (like weak encryption or configuration, certificate or account takeover, or insufficient cybersecurity systems) to gain unauthorized access to a victim’ s network, systems, or devices. Breaches are representative of a physical crime like burglary. In cybercrime, a Breach is often a policy violation (per a company’ s terms of service or other policies) but is not typically codified as a crime.
- (C)ompromise: Compromises are the leveraging of access to a victim’ s network, systems, or devices to achieve objectives including data theft, extortion (via ransomware), or system disruption. Compromises are representative of a physical crime like theft, fraud, embezzlement, or destruction of property.

With Attacks, access brokers violate the Computer Fraud and Abuse Act by abusing access and manipulating credentials to attack a computer, maintain access, and sell that access. The cybercriminals that purchase access from brokers also commit crimes when they Compromise victim systems to steal information or commit extortion. However, APT actors that Breach systems and exercise access without manipulating or changing the environment are only guilty of accessing the environment. There’ s a clear crime committed in the Attack and the Compromise, but not in the Breach. It is very difficult to prosecute a persistent threat actor who is benefitting from access to facilitate a third party with a compromise interest. In addition, law enforcement often charges cyber crimes incorrectly. Since prosecutors work with the charges they’ re given, charges that don’ t stand up to a statute are unlikely to lead to consequences for cybercriminals.

These compounding challenges show the complexities of cyber incidents and the necessity for both cybercrime investigators and cybersecurity professionals to coordinate the investigation and prosecution of cybercrimes.

Case study: The Complexity of a Cybercrime

A cybercrime investigator was hired to investigate a case in which a company CFO was recorded authorizing transactions that appeared to be embezzlement. The CFO, who reported the incident and requested an investigation, claimed he didn' t know how the payments had been made.

The investigator first analyzed network logs and found that an IT administrator had used a password sniffer to capture encrypted credentials between the CFO' s computer and the financial system. The administrator had then used freeware to crack the password and create invoices via a RDP session on the CFO' s computer. Upon further investigation, it was also found that the payments were being routed to an offshore account for a fake entity for the same IT administrator.

The investigator further analyzed the transactions and identified that the CFO' s credentials were associated with both creating invoices and authorizing the payments. This raised suspicions, as CFOs don't typically create invoices themselves- an accounts payable clerk performs that task and payments usually involve two people to ensure integrity. After interviewing the company' s IT staff, the investigator learned that a current IT administrator was previously an auditor who was familiar with accounting procedures- the suspect was identified and the investigator alerted relevant law enforcement officials. Law enforcement interrogated the administrator and analyzed his home computer, at which point the administrator confessed to the crime.

What had initially looked like embezzlement by the CFO had in fact been theft by the administrator. The investigation had also revealed that the company lacked two factor authentication, alerts associated with the CFO posting a payment without a second party' s approval, and other security measures. This case study demonstrates both how the initial impression of a crime may not tell the full story and how organizations must institute strong security measures to avoid giving criminals the opportunity to commit crime.

Chapter 3

Artifacts of Cybercrime

Introduction

Every crime leaves evidence behind. A crime is not a single act but a series of activities that culminates in an illegal action. Consequently, traces and clues that reflect the planning, organization, conduct, and commission of cybercrime are available if the "Tools, Tactics, and Procedures" (TTP' s) are understood by investigators and organizational managers. Whether committed as a random or a planned act, those traces will help to distinguish the nature of the crime. Such traces are commonly referred to as "indicators" and "artifacts".

In the context of cybercrime investigations, the differences between indicators and artifacts are as follows:

Indicators of Compromise (IoC) and Indicators of Attack (IoA)

- Indicators of Compromise (IoC) are behaviors or data that indicate a data breach, intrusion, or cyberattack has occurred. They are critical in identifying system vulnerabilities and confirming cyberattack occurrences.
- Indicators of Attack (IoA) focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack.

Artifacts

- Digital artifacts are items that get left behind based on the activities of the end user. They are better indicators of what actually transpired and can reveal details that content never will, such as the intent or state-of-mind of the individual.

Indicators of compromise and attack are used to confirm cyberattack occurrences and detect the intent of an attacker, while artifacts are better indicators of what actually transpired and can reveal more information than content alone. Indicators are observed through activity monitoring: of network, endpoint, and identity services and device usage. Artifacts are discovered through behavioral analysis of such indicators, and digital forensic examinations of related equipment and logs.

Over the last 10 years, there have been a number of trends in how organizations create, manage, maintain, and curate the intelligence used to detect and respond to both Indicators of Compromise and Indicators of Attack:

- Increased Sophistication: IoCs have become more sophisticated and comprehensive, encompassing various types of indicators beyond just IP addresses, domains, and file hashes. Today, IoCs often include more esoteric indicators such as Mutex[77], Imphash[78], and Fuzzy Hash[79] along with behavioral patterns, tactics, techniques, and procedures (TTPs), and contextual information about threat actors and their motivations.

[77] Lenny Zeltser - "Looking at Mutex Objects for Malware Discovery & Indicators of Compromise" https://www.sans.org/blog/looking-at-mutex-objects-for-malware-discovery-indicators-of-compromise/

[78] Mandiant - "Tracking Malware with Import Hashing" https://www.mandiant.com/resources/blog/tracking-malware-import-hashing

[79] Niklolaos Sarantinos et al - "Forensic Malware Analysis: The Value of Fuzzy Hashing Algorithms in Identifying Similarities" https://ieeexplore.ieee.org/document/7847157

- Integration with Threat Intelligence Platforms: The integration of IoCs with threat intelligence platforms has become commonplace in organizations, enabling access to curated IoCs from trusted sources and their incorporation into security infrastructure. Proactive threat hunting, real-time alerting, and automated response actions are increasingly facilitated by IoCs.

- Emphasis on Contextual Analysis: There is a growing emphasis on the contextual analysis of IoCs to distinguish between legitimate and malicious indicators. Contextual analysis involves correlating IoCs with additional data sources such as network traffic logs, endpoint telemetry, and user behavior analytics to accurately determine the severity and relevance of potential threats.

- Sharing and Collaboration: The sharing of IoCs among organizations, between industry sectors, and across national boundaries has improved collaboration and collective defense against cyber threats. Initiatives like Information Sharing and Analysis Centers (ISACs) and government-sponsored threat intelligence sharing programs facilitate the exchange of IoCs and actionable intelligence to strengthen cybersecurity posture globally.

- Focus on Threat Hunting: IoCs play a critical role in proactive threat hunting activities where security teams actively search for signs of compromise within their networks. By leveraging IoCs as starting points for investigations, organizations can uncover stealthy threats and vulnerabilities that may evade traditional detection mechanisms.

However, there are possible drawbacks to IoC use :

- Over-reliance on Known Indicators: IoCs are primarily based on known patterns of malicious activity, and may not detect novel or previously unseen threats. Sophisticated adversaries can evade detection by modifying their tactics, techniques, and procedures (TTPs) or by using custom-built malware and related infrastructure that are not represented by known IoCs.

- False Positives and Negatives: IoCs can generate false positives (incorrectly identifying benign activities as malicious) or false negatives (failing to detect actual threats), leading to alert fatigue and inefficiencies in incident response. The dynamic nature of IoCs requires continuous tuning and validation to minimize false alarms and ensure accurate detection.

- Limited Scope: IoCs provide a snapshot of specific indicators associated with known threats but may lack broader context or intelligence about the motivations, tactics, and objectives of an adversary. IoC-based detection should be complemented with threat intelligence analysis and a contextual understanding of cybersecurity risks to overcome this limitation.

- IoC Staleness: IoCs have a limited lifespan as threat actors frequently change tactics and infrastructure to evade detection. Stale IoCs may no longer be relevant or effective in identifying emerging threats, necessitating continuous updates and the enrichment of threat intelligence feeds. This curation process can be challenging, and effort must be applied to ensure the validity of the Indicators in use.

- Privacy and Legal Concerns: Sharing IoCs, particularly those containing personally identifiable information (PII) or sensitive data, may raise privacy and legal concerns, especially in regulated industries or jurisdictions with stringent data protection regulations. Organizations must adhere to applicable privacy laws and information sharing agreements when exchanging IoCs with external parties.

While IoCs remain a valuable component of cybersecurity defenses, their effective utilization requires a balanced approach that considers their strengths, limitations, and the broader threat landscape.

This chapter will articulate the artifacts of cybercrime available to assess as evidence of the stage of activities, as indicators or attributes of the involved activities of the crime. Internal and external sources of information to help investigators discover such artifacts will be described – to also assist organizational policymakers and managers to build inclusive audit and assessment programs, or defensive and protective systems and procedures.

At the conclusion of this chapter, readers will have understanding of:

- What are the indicators of cybercrime?
- How do artifacts differ from indicators of cybercrime?
- What are the stages of cybercrime activities?
- What types of cybercrime artifacts are available to investigators?
- Where can investigators find cybercrime artifacts and indicators?

Topic in Artifacts of Cybercrime

Figure 3-1 displays topic categories in the "Artifacts of Cybercrimes" knowledge domain.

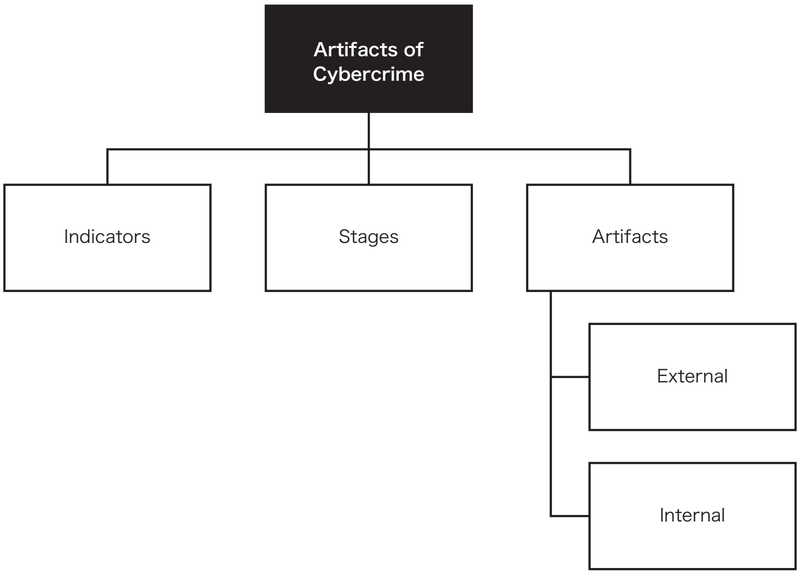


Figure 3-1. Topic Categories in the "Artifacts of Cybercrimes" knowledge domain

What are Indicators of Cybercrime?

Artifacts and evidence are interrelated terms but do not refer to the same thing. An artifact is something that is created by “doing” something – such as a Microsoft Word document, the meta data that relates to the document, and/or the registry entries concerning the users’ creation and use history of the document. Evidence on the other hand is the collection of artifacts that describes “how” the artifact(s) relate to an issue, such as copying protected information from one file into a document on a removable media drive.

Artifacts of cybercrime can be isolated and independent, or can be correlated and interdependent. They may exist in structured or unstructured technical locations – such as contents of a computer disk; or may be the result of (documented) human interactions – such as notes or video recordings.

Artifacts of a cybercrime reveal the resources and methods used to perform related activities. Associated to those therefore are indicators relating to the stage and objective of the activities. There are accordingly available external and internal artifacts that should be collected from sources (to be described in Chapter 5) as evidence.

Most technical analysts and cybercrimes investigators focus on the micro level of attacks, meaning they look for the files, internet addresses, domain names, hash values or other identifiers that result from the successful exploitation of a target. These indicators of an exploitation are typically referred to as IOC’ s or “Indicators of Cybercrime”. However, these technical analysts are focused on the micro scale because their area of authority, or sometimes their experience and knowledge, is limited just to those systems they have been tasked to defend and investigate. Cyber investigators should recognize that the area of authority is much larger and the requisite field of knowledge must include the macro as well as the micro.

This means that it is important first to understand the larger framework that preexisted the commission of a cybercrime. The planning, preparation and execution that occurs during cybercrime activities leaves its own indicators across the wider Internet (how wide depends upon the scope of the cybercrime) that can be referred to as Indicators of Cybercrime or IOC’ s. Such indicators go far beyond the exploitation of a single target and if discovered can help analysts understand the scope and assets of the person(s) or group(s) that orchestrated the crime, or the scope of affected victim(s) systems or personnel.

Indicators of Cybercrime refer to activities that artifacts relate to. The most common framework used to describe (similar) indicators was developed by Lockheed Martin Corporation and is called the “Cyber Kill Chain”.[80] That model associates activities that an attacker will perform from initial target identification – through to achieving their objectives.

[80] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, Ph.D., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Available at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

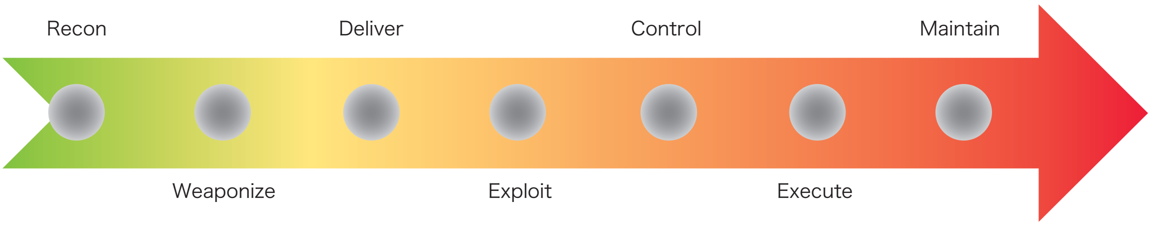


Figure 3-2. Cyber "Kill Chain" Model[81]

The Cyber Kill Chain model is an effective way to demonstrate sequential events occurring as a consequence of a single actor, or even an organization; however, as cybercrime organizations have evolved, as well as the profiles of cybercriminals previously described in Chapter 2 – the Cyber Kill Chain becomes less specifically relevant. Although the model describes activities, it fails to represent the organization(s) and objectives of the activities. Today' s cybercrimes may involve individuals or several independent or interdependent organizations to achieve objectives of a cybercrime. Similarly, the target of a cybercrime may simply be the attacked target, or may include their customers and/or partners. As much of the attack and reconnaissance activities today are performed by third parties, and compromise activities are often "farmed out" to skilled technical labor sources – there may be several coincidental actors performing disparate or discrete actions to achieve their own objectives.

Because of the complexity of cybercrimes, their organization, methods, and profiles (according to interests/objectives) – a new model that separates Indicators from the activities that are performed in achieving "stages" of cybercrime can be considered as the following diagram.

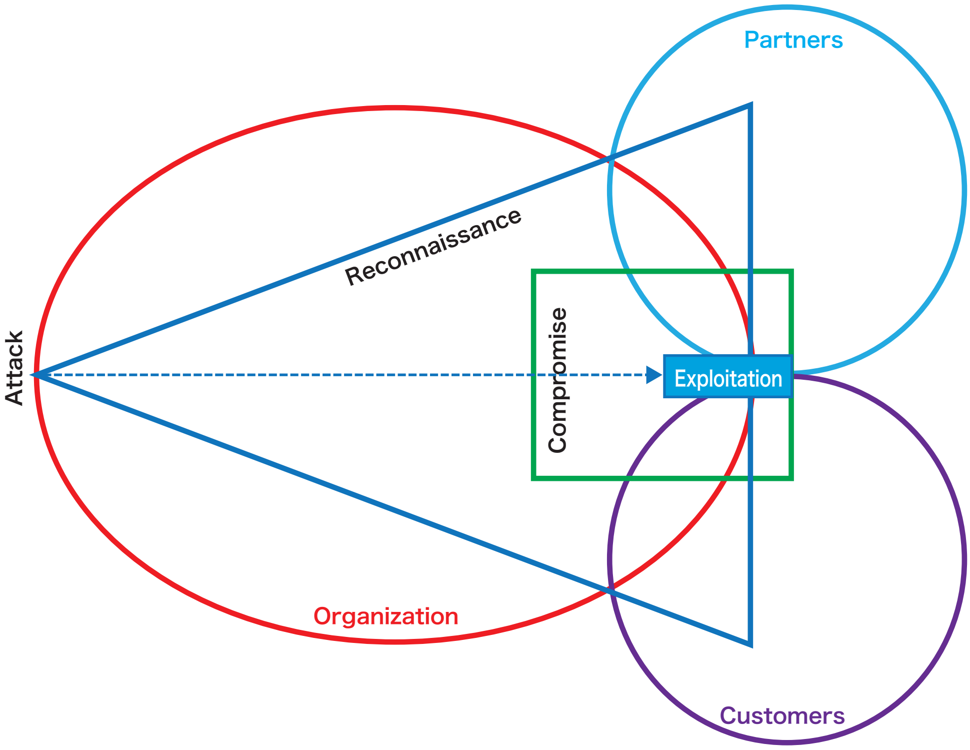


Figure 3-3. Cybercrime Indicators

[81] The "Cyber Kill Chain" is trademarked by Lockheed Martin Corporation

Indicators of Cybercrime refer to methods of successfully achieving objectives at each “stage” of a cybercrime. Different actors will have different objectives. For example, a criminal intent on financial fraud from a bank payment network may employ hackers to target and provide access to a bank, along with and different rogue banking technicians to exploit that access by mimicking bank procedures, and offshore bank accounts to launder funds stolen via illicit funds transfers. Each of the actors in that scenario are committing cybercrimes, and each takes has steps to achieving goals of stages of the ultimate cybercrime (the fraud).; However, related indicators of compromise (a different concept that refers to purely technical artifacts found in computers) are as unique as the different actors (although sometimes different actors accidentally or coincidentally at least employ coincidental botnet infrastructures). The complexity of today' s cybercrimes means that it is very difficult therefore to attribute the crime to an actor, unless the indicators and stages of activities are understood from investigation.

Additional and alternative models to map and manage the different phases of Cyber Attack and Defense have come into widespread use in the last decade. Notably, the MITRE ATT&CK[82] and D3FEND[83] models, which focus on offensive techniques and countermeasures respectively, must be acknowledged.

The MITRE Corporation[84] has developed two complementary frameworks designed to assist in understanding and improving cybersecurity defenses: the ATT&CK and D3FEND frameworks. These frameworks provide a structured way to identify and mitigate cyber threats, offering valuable guidance for cybersecurity professionals.

MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used as a foundation for the development of specific threat models and methodologies in the private sector, government, and cybersecurity product and service community. The framework is designed to provide a common taxonomy for cybersecurity practices, enabling a more structured approach to threat detection, analysis, and response. It offers the following details:

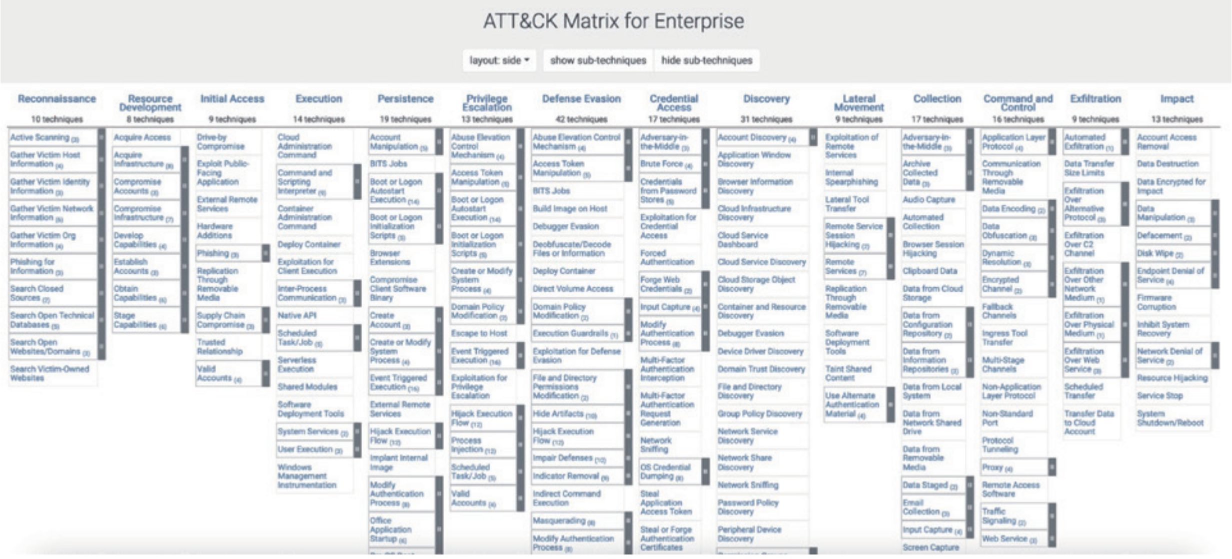
- Tactics and Techniques: The actions of adversaries are categorized into tactics, representing the objectives they are trying to achieve, and techniques, detailing how they achieve these objectives. This categorization helps defenders understand the "how" and "why" behind the actions of adversaries.
- Matrices: Various matrices for different environments are covered, such as Enterprise, Mobile, and Cloud. Each matrix focuses on specific aspects of its environment, allowing for more targeted security measures.
- Mitigations: For each technique, mitigations are suggested to help prevent or limit the effectiveness of that technique. These mitigations are practical measures that organizations can implement to improve their security posture.
- Groups and Software: Information on known adversary groups and the software they commonly

[82] https://attack.mitre.org/

[83] https://d3fend.mitre.org/

[84] https://www.mitre.org/

use is included, helping defenders identify and attribute attacks.



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (3)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			Software Deployment Tools	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			System Services (2)	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			User Execution (3)	Modify Authentication Process (8)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
			Windows Management Instrumentation	Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Network Service Discovery		Email Collection (3)	Remote Access Software		
						Impair Defenses (10)		Network Share Discovery		Input Capture (4)	Traffic Signaling (2)		
						Indicator Removal (9)		Network Sniffing		Screen Capture	Web Service (3)		
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (8)		Peripheral Device Discovery					
						Modify Authentication Process (8)							

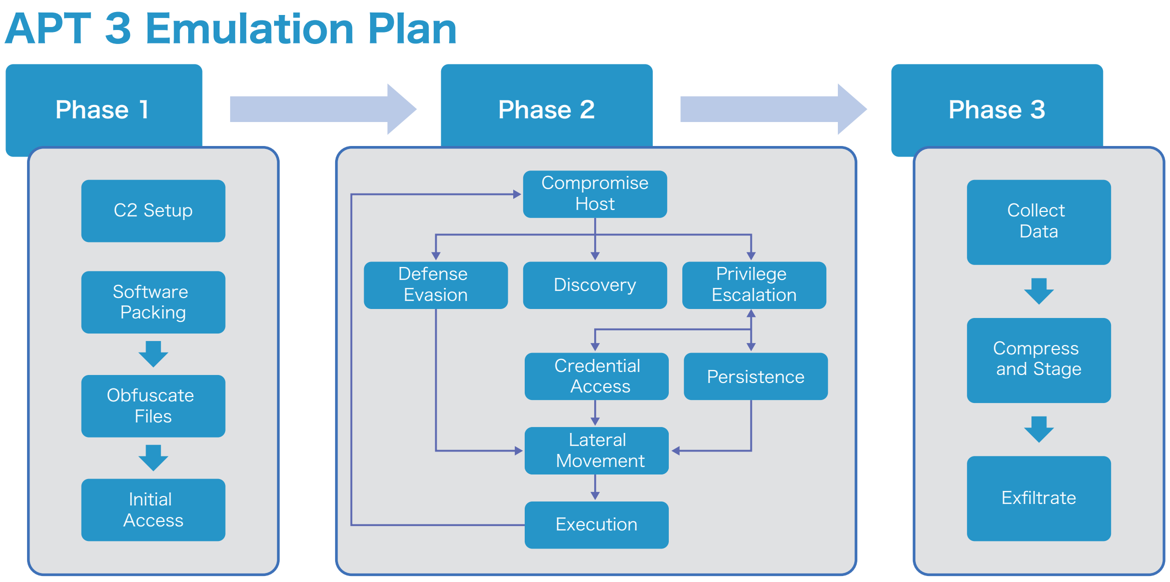
Figure 3-4. Illustration of the depth of detail in the Mitre ATT&CK$^{(TM)}$ framework

Adversary Emulation Plans

To demonstrate the value of ATT&CK for both offensive teams and defenders, MITRE has developed Adversary Emulation Plans[85]. These documents serve as blueprints, illustrating potential applications of publicly accessible threat intelligence and ATT&CK frameworks. The goal of these plans is to enhance network and defense testing by empowering red teams to replicate adversary tactics more effectively, as outlined by ATT&CK. This initiative contributes to a broader effort aimed at improving product and environment testing, along with developing ATT&CK behavior analytics, moving beyond the narrow focus on specific indicators of compromise (IOC) or tools.

Current threat intelligence reports often emphasize malware analysis, initial breaches, and command and control (C2) strategies. However, detailed insights into how attackers link techniques or conduct operations directly from the keyboard are scarce. These emulation plans, constructed from available threat intelligence, inherit such limitations. To address this gap, the following approach is offered to integrate ATT&CK tactics, drawing from comprehensive red teaming experiences. In developing these plans, specific Advanced Persistent Threat (APT) groups cataloged in ATT&CK were analyzed to explore potential emulation strategies for those APTs. This process involved identifying the functionalities of the tools used by an APT and suggesting alternative methods to mimic those actions. The aim is to allow operators to mirror the general modus operandi of particular adversaries—adhering to their documented tactics, techniques, and procedures (TTPs) and behaviors—while permitting some flexibility in the execution. Further support is provided through a 'cheat sheet' of commands applicable for analogous actions across popular red teaming platforms. The following high-level diagram offers a framework for structuring an APT3 emulation strategy.

[85] https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/adversary-emulation-library/



Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved MITRE

Figure 3-4. Sample Adversary Emulation Plan

Example emulation plans are available from MITRE and offer insight into the approach and methodologies employed by different threat actors.[86]

MITRE D3FEND Framework

MITRE D3FEND is a complementary framework that focuses on cybersecurity countermeasures. While ATT&CK outlines how attackers operate, D3FEND provides information on how to defend against those actions. It is designed to enhance the cybersecurity posture of organizations by detailing defensive techniques that mitigate or prevent the tactics and techniques listed in ATT&CK. It offers the following details:

- Countermeasure Techniques: Countermeasures are listed in a structured format, similar to how ATT&CK lists attack techniques. These countermeasures are mapped directly against ATT&CK techniques, providing a clear guide on how to defend against specific adversary behaviors.
- Taxonomy: A taxonomy of cybersecurity countermeasures is introduced, categorizing areas such as Harden, Detect, Isolate, Deceive, and Evict. This categorization assists in planning and implementing a comprehensive cybersecurity strategy.
- Technical Specificity: Technical detail on the implementation and effectiveness of various countermeasures is provided, offering guidance on how they can be applied in different contexts.

Together, the ATT&CK and D3FEND frameworks offer a comprehensive approach to understanding and combating cyber threats. By detailing specific adversary behaviors and corresponding defense measures, they enable cybersecurity experts to better plan, implement, and evaluate cybersecurity strategies.

[86] https://attack.mitre.org/groups/G0022/

Artifacts

Technical artifacts that relate to indicators of compromise can change rapidly as criminals change something as simple as which internet address a victim communicates with or the name of a file, to avoid detection. Indicators of cybercrime are left across systems that criminals have made use of and are captured by monitoring systems and historical records – including both public systems such as the Internet and private systems such as personal or corporate computers. IOCcs are created by related artifacts each time a cybercrime is committed, and are preserved regardless of the future changes that the criminal may make. It is the overlap between IOCcs that allows us to begin the process of attributing a campaign to a criminal entity, by focusing investigation on the crime and not individual artifacts.

To put this in terms of real-world organized crime, a campaign could be compared to traditional crimes. For instance, if an organized crime group was involved in Vice, Kidnapping or Extortion those would be three individual campaigns committed by one group. The indicators for each type of crime would be different because the execution of the crime varies, but there will be shared components such as people, transportation and infrastructure that may be shared between them. The same is true in the world of cybercrime if a group is involved in Ransomware, Credit card theft and Espionage. There may be different indicators for each of the crimes, but they may also share commonalities that allow grouping to reveal organized activities.

Attack

Depending on the objectives of the campaign, the method of attack will vary. Prior to any other action performed, the attackers must have an objective in mind and means to achieve it. For instance, if an attacker was financially motivated and looking for the widest possible reach, they might plan an ad-based attack that would target anyone accessing popular websites with hostile ads. In more targeted scenarios where they were only interested in a specific company, attackers would more likely utilize research and social engineering to gather email addresses of known employees and/or determine what topics would be most compelling for employees to click on via spear-phishing links.

More advanced attackers may research the hardware their target has purchased or the companies they' ve announced partnerships with, fund the development of new exploits (called zero days) that can be used to compromise the external network, and then move inward. Attacks are considered indicators because the nature of the targeting mechanism will let us know:

1. Was this targeted at a specific organization or did it cast a wide net?
2. What was the target of the attack (user groups, countries, etc.)?
3. What was the motivation of the group?
    a. Financial Gain (Ransomware, Payment Card Theft, Credential Theft)
    b. Espionage (Targeted attack with long term remote access and exfiltration)
    c. Sabotage (Deletion and disabling of services and servers)
    d. Hacktivism (Defacement or denial of service)

Reconnaissance

Indicators of cybercrime can be found in multiple sources (to be detailed in Chapter 5) depending on how the attacker collects information about their target(s). Cyber-reconnaissance used to be thought of as simply probing the perimeter defenses of a target to determine its weaknesses. Today, with the huge amount of publicly-available data about companies and their employees, locations, and technologies used, an attacker can quickly develop knowledge about possible weaknesses before ever committing to their activities.

Compromise

The act of compromise is where most people begin looking for indications and artifacts of cybercrime, as it is the most understood and recognizable (and visible) activity to the victim organization. Depending on the type of cybercrime, indicators of compromise activities may be devised that allow an organization to search for affected systems and applications – once reliable “signatures” are discovered. Antivirus and antimalware companies as well as Intrusion Prevention and Network Monitoring technologies provide the ability to detect indications of previously seen attacker activity, sometimes also allowing you to determine which campaign(s) the activity might correlate with.

Aside from technical indicators, though, the level of sophistication of the attacker and their apparent habits are useful indicators as well. Commodity malware is widely used by (and sold to) criminal organizations; however, unique malware with levels of sophistication that reflect well-funded and organized groups sometimes appears. In such cases, it can be assumed that the attack was targeted and a more significant purpose exists for the campaign than simply expanding botnets.

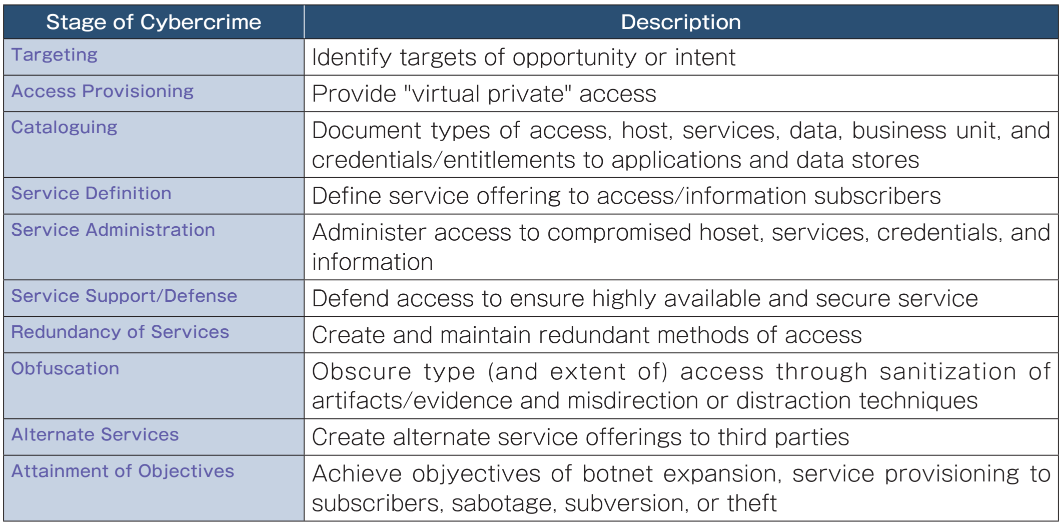
Exploitation/Success

Exploitation is the hardest category to predict until the impact is determinable. Exploitation means that the attacker has successfully gained entry, explored their options, and executed their objective(s) (financial theft, espionage, sabotage, etc.). Exploitation objectives may be simple: if a large number of systems on the victim network become unusable due to ransomware, then the objective was extortion or sabotage. If large amounts of data have been stolen from a victim network, then the objective was espionage (industrial or nation state) or theft. As discussed in Chapters 1 and 2, the apparent compromise activities may distract from understanding the objective that the criminal actually had. There are many objectives, as there are many different criminal groups in operation in the world. The question an investigator must ask themselves is “why”? Ultimately, what was their interest, how did they pursue it, and who benefits?

Stages of Cybercrime Activities

The following stages include component activities that occur during commission of cybercrimes. The artifacts related to these activities should be assessed in context to the related description. As previously described, these activities may be independent, redundant, or coordinated according to the profile and interests/objectives of the cybercriminal or organization that performs them. These activities are similar to the Cyber Kill Chain previously described in Figure 3-2; however, they are expanded to relate to how cybercrimes have evolved into a “shared services” economy of scale and operation – whether within a single organization or by inter-dependent cybercriminal interests.

Figure 3-5. Cybercrime Activities



Stage of Cybercrime	Description
Targeting	Identify targets of opportunity or intent
Access Provisioning	Provide "virtual private" access
Cataloguing	Document types of access, host, services, data, business unit, and credentials/entitlements to applications and data stores
Service Definition	Define service offering to access/information subscribers
Service Administration	Administer access to compromised hoset, services, credentials, and information
Service Support/Defense	Defend access to ensure highly available and secure service
Redundancy of Services	Create and maintain redundant methods of access
Obfuscation	Obscure type (and extent of) access through sanitization of artifacts/evidence and misdirection or distraction techniques
Alternate Services	Create alternate service offerings to third parties
Attainment of Objectives	Achieve objyectives of botnet expansion, service provisioning to subscribers, sabotage, subversion, or theft

Targeting

Targeting involves the criminal organization deciding which victims will ultimately yield the best result. For commodity malware (Ransomware, Credential Theft, Botnet farming) this may be less about direct targeting and more about identifying which mechanism gathers the most targets (Spam, Phishing, malicious advertisements). For targeted attacks related to espionage, payment card theft, or wire fraud, this becomes more specific as the attacker is identifying which victims will yield the best result for their effort - in the form of monetary benefit for the sale of information stolen or monies transferred.

Access Provisioning

When provisioning access, the cybercriminal must create or lease some kind of infrastructure that will provide “virtual private network” access to their needs (or their subscribers). Many people misunderstand command and control communications to mean that any communications from hostile foreign countries are attacker infrastructure when,with the advent of public cloud computing and worldwide hosting services, any network could be facilitating or providing access to target victims. This becomes an even greater problem when the attacker makes use of an already compromised system, assumed to be a good actor, to host their own malicious infrastructure. Some estimate as many as 70% of botnet controlled computers are “behind corporate firewalls”, meaning that of known C2 networks – the majority of related systems are already compromised and exist in controlled environments. Those systems can provide access on-demand.

Cataloguing

As cybercriminals successfully gain access to targeted hosts, they document the type of access and services available on that host. The “catalog” of related hosts may be developed for proprietary purposes (similar to an asset management database developed and used by organizational IT administrators), but it may also be offered to subscribers – in whole or in part. Increasingly, botnet expansions are performed by third-party actors seeking to sell compromised host access to subscribers with competitive interests. The host type, build and configuration of services, credentials, and entitlements to organizational resources are each valuable commodities in related catalogs.

Service Definition

As an actor determines the access they have – to hosts, services, applications, credentials, the organization, partners, and/or customers – they will define the type of service they choose to build in the compromised host or estate. Initially the service will simply be remote access, but thereafter it will evolve according to their own or subscriber interests to include more advanced services.

Service Administration

As cybercriminals successfully gain access and develop their catalog (and service offerings), they must administer the access that is provided to subscribers - just like any other information technology resource. As the infrastructure grows, the systems will need to be maintained and resources added and patched. Because of this, if the attacker' s infrastructure is seized it may reveal information about the attacker' s identity, objectives, and organization.

Service Support/Defense

As the cybercriminals' infrastructure grows and is detected by security tools and researchers, there will be times when victim organizations and vigilantes attempt to retaliate against the attackers. The criminals will defend their own infrastructure from attack from victims, vigilantes, and other attackers.

Redundancy of Services

Many malicious software packages today are commercially supported through the criminal networks that provide them. They grow in sophistication and capability on a daily basis. Cybercriminals will create redundancy of service with custom tools such as malware, and will also seek to exploit and reconfigure existing services to ensure access and management of their services is available.

This means that the old approach of simply denying access to a specific internet address is no longer enough to prevent a cybercriminal from continuing their access. Often it is more important to identify the varied methods and means of communication that a cybercriminal utilizes than it is to immediately block access to the command and control communications network (addresses). In response activities, this may place the investigator at odds with the victim organization who wants to halt all access that the cybercriminal has; however, until the scope of the activities and capabilities are understood, no effective response can be ensured.

Obfuscation

One of the capabilities that cybercriminals have continued to mature is that of obfuscation. This involves taking what is plainly malicious software or network traffic and hiding it within other data to make it appear benign or unreadable. This could be as simple as encoding the data with a common scheme (like Base64[87]), rotational ciphers (such as ROT13[88]) or actual public key cryptography (such as PGP[89]) to protect the malicious software from being understood. The same is true for the network

[87] https://tools.ietf.org/html/rfc4648

[88] http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf

[89] http://www.pgpi.org/doc/pgpintro/

traffic generated by the cybercriminals' infrastructure that could be made to look like domain name translation requests, regular webpage access, or the utilization of legitimate services like Dropbox, Gmail or others, for command and control communications.

Alternate Services

Cybercriminals will often compromise a victim for a specific campaign and reach their objective only to find they still have useful access afterwards. In these cases, the cybercriminal may choose to stay dormant until a new campaign is launched for a new objective or they may sell the access to another criminal organization for their own objectives. Once again, different attackers may make use of a variety of services aside from what has been seen before. This includes creative solutions such as victim or surrounding infrastructure wireless or inter-connected application services that obfuscate their activities (and tools) and ensure that any network traffic generated by their actions is never seen on the victim network.

Attainment of Objectives

The last stage occurs when the attacker has achieved their objective(s). Depending on the type of cybercrime that occurred, this may be obvious to the victim (Ransomware, Sabotage, Theft, etc.). They may learn about it from third party sources such as vendors, partners or journalists; or they may never know it occurred at all. It is not unusual to find victims that have been compromised by the same criminal organization for over 3 years with the victim never aware that several campaigns have succeeded.

"Living off the Land"

One cybercrime trend worth noting is the use of existing, legitimate tools in the environment to perpetrate attacks and move laterally within an organization. Known as "Living off the Land" attacks or "LOTL"[90], these are fileless methods- meaning there is no need to install any code or scripts within the target system. Native tools that can be utilized in this way include PowerShell and Windows Management Instrumentation, among others.

Malicious software embedded in the Windows registry, known as resident registry malware, is capable of inserting malicious code directly into the system's registry. It can be programmed to initiate upon the startup of the operating system, ensuring persistence and remaining undetected for extended periods. Memory-only malware, on the other hand, operates solely within the system's memory, evading detection while serving as a covert entry point for various malicious activities such as reconnaissance, lateral movement, and data exfiltration.

In the realm of ransomware tactics, fileless techniques are employed as a primary method to infiltrate systems. By implanting malicious code into documents and leveraging legitimate software tools, attacks are executed, encrypting files and causing significant disruptions. Among the arsenal of

[90] https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/threat-actors-leverage-legitimate-tools-in-lotl-attacks

tools favored by ransomware groups are PowerShell, PsExec, Windows Management Instrumentation (WMI), Mimikatz, and Cobalt Strike.

LOTL threat actors resort to stealing legitimate user credentials to perpetrate business email compromise scams. These scams aim to pilfer sensitive information including account credentials to conduct reconnaissance on additional systems, hijack legitimate tools, and establish persistent access for further malicious activities.

"LOLBins" stands for "Living Off The Land Binaries" and refers to legitimate, non-malicious system tools that are native to the operating system (OS) and commonly used applications that attackers can abuse to perform malicious activities while evading detection. The term can also be extended to include "LOLScripts," which refers to scripts and batch files that can be similarly misused. These concepts are related to broader "Living Off The Land" tactics, where, as mentioned previously, attackers use legitimate pre-installed tools to conduct their operations, making it harder for security systems to detect their malicious activities.

Key Features of LOLBins

- Evasion and Stealth: Attackers can blend in with normal network activity, making their actions look less suspicious to security tools and system administrators. This method reduces the likelihood of detection compared to using custom malware, which might be flagged by antivirus software.
- Functionality Abuse: A wide range of functions useful to attackers can be performed, including but not limited to file download, execution, persistence establishment, privilege escalation, defense evasion, and data exfiltration. For example, Windows Command Prompt (cmd.exe) and PowerShell (powershell.exe) are powerful tools that can execute scripts, download files from the internet, and modify system settings.
- No Need for External Tools: Since LOLBins are either already present in the systems or are commonly installed applications, attackers don't need to upload any tools, decreasing their footprint and the chance of being caught by traditional antivirus or endpoint detection and response (EDR) systems.
- Challenges for Defenders: The legitimate nature of these tools presents a challenge for defenders, as blocking or limiting them could disrupt normal system or user operations. This necessitates more sophisticated detection techniques that focus on behavioral analysis and context to distinguish between legitimate and malicious use.

Commonly Used LOLBins:

- Windows: Cmd.exe, PowerShell (powershell.exe), Certutil.exe (for downloading or decoding files), Bitsadmin.exe (for background file transfers), and Regsvr32.exe (to execute code and bypass user account control).
- Linux/Unix: Curl or Wget (for downloading files), Cron (for scheduling tasks), and Bash (for executing scripts and commands).
- macOS: Osascript (for executing AppleScripts and other scripts), Curl/Wget, and Launchd (for persistence).

LOLBin Risk Mitigation and Threat Detection:

Mitigating the risk of LOLBin abuse involves a combination of strategies including strict application whitelisting, monitoring and logging process execution paths and command-line arguments, employing behavioral detection strategies, and educating users about phishing and other tactics attackers use to gain initial access. Detection and response strategies must also be adjusted according to evolving attacker tactics.

LOLBins have been utilized in several high-profile cyber breaches and attacks. Their usage is often not the centerpiece of reports, but plenty of document exists of attackers leveraging these tools for various stages of attacks. Here are a few examples:

- WannaCry Ransomware Attack (2017): While the primary method of propagation and damage was through the EternalBlue exploit and the DoublePulsar backdoor, the WannaCry ransomware attack also leveraged built-in Windows tools for its operations. For instance, it used vssadmin to delete shadow copies and backups to prevent file recovery. This is a common tactic used by ransomware actors to increase the pressure on victims to pay a ransom.
- SolarWinds Orion Supply Chain Attack (2020): In this sophisticated and wide-reaching attack, adversaries compromised the build system of SolarWinds' Orion software, inserting malicious code into updates that were then distributed to customers. During the post-compromise stages, attackers used various LOLBins such as PowerShell to execute commands, move laterally, and exfiltrate data without triggering alerts from security tools that were monitoring for traditional malware signatures.
- NotPetya Attack (2017): NotPetya was a destructive malware outbreak that used the EternalBlue exploit for initial infection. Following infection, it utilized LOLBins such as PsExec (a legitimate Microsoft tool) and WMIC (Windows Management Instrumentation Command-line) for lateral movement and to spread across networks. By using these tools, attackers were able to execute the malware via system privileges on remote machines.
- Stuxnet (Discovered in 2010): Stuxnet, the cyberweapon targeted at Iran's nuclear program, used legitimate Windows functions and features (such as LNK files and print spooler services) to spread and execute its payload. While these are not standalone binaries, they reflect the broader LOTL strategy of to avoid detection.
- APT29/Cozy Bear Campaigns: APT29, a threat group attributed to the Russian government, has been reported to use various LOLBins in their cyber espionage campaigns. Tools like certutil.exe have been used to download malicious payloads and PowerShell has been extensively used for the execution of in-memory payloads, data collection, and exfiltration, often leveraging encoded commands to obfuscate activities.

These examples illustrate the versatility and stealthiness the use ofLOLBins enables in cyber attacks. The use of native tooling to enable and expedite attacks can make the application of IoCs and artifacts more challenging for blue teams and network defenders. This underscores the challenge defenders face in distinguishing between legitimate and malicious uses of these tools, and the necessity for advanced monitoring and analytical capabilities to detect anomalous behaviors indicative of an attack.

Artifacts of Cybercrime

“Artifacts” can be a difficult term to understand. They are not evidence, nor are they simply indicators. They are found in sources, but are discrete objects that have been created by human, computer, or combined interactions in cybercrime activities. Artifacts are divided into two categories: those external to the victim' s computer network and those contained within the victim' s computer network as a result of the criminal' s actions.

Indicators of cybercrime reflect the intentions of criminals, while artifacts represent the residue of their actions – notes, fragments of files or communications, recordings, messages, caches of forgotten (Dark) web pages that are no longer in service, or etc. The combination of indicators and artifacts lead to evidence of the crimes that have been pursued or committed by cyber criminals.

The following figure demonstrates the association of indicators to artifacts, evidence, and sources (which will be described in Chapter 5).

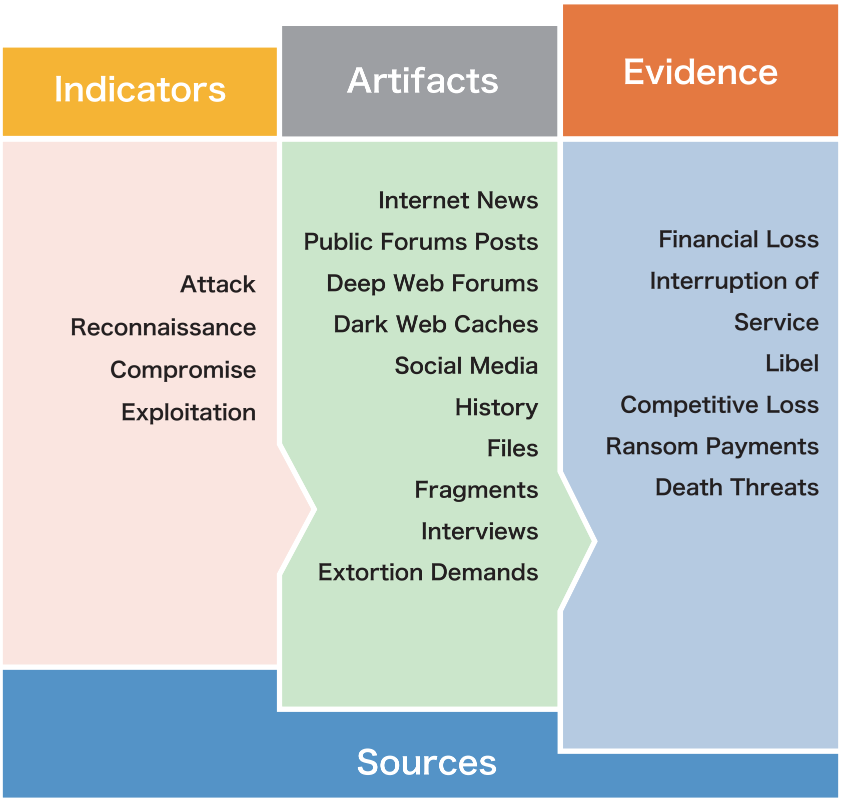


Figure 3-6. Association of Indicators to Artifacts

External Artifacts

External artifacts are sources of evidence or intelligence that exist outside of the victim' s network. Organizations may be actively collecting intelligence in regards to what indicators and artifacts exist from related sources. Threat Intelligence companies collect data from technical and market information sources and sell the data to organizations to allow them to understand emergent threats and active campaigns. In addition to these private sources, confidential informants (such as hired security researchers) and undercover operatives who are monitoring data sources (such as deep web sites, marketplaces and chat rooms) may produce useful artifacts of cybercrime activities.

The Internet

The Internet represents publicly-accessible areas of the worldwide web captured by Internet search engines such as Google and Bing. Historical records of who purchased an internet address or domain name exist by companies such as domaintools.com as well as "WHOIS[91]" records indicating where those services were physically hosted. These services reveal one of the few artifacts in the investigative trail where an attacker may have had to make a payment using some form of currency. As in every other real-world investigation involving payments, once a transfer or payment has taken place it can be "tracked-back" to the source and an attempt to unravel the connections can begin. Notably, the rise of cryptocurrency in the last decade has offered criminal actors significant capabilities and tools to evade and bypass investigative efforts, allowing the transfer and movement of funds with a high degree of anonymity.

Deep Web

The deep web represents all of the parts of the public internet that cannot be reached by services such as Google index and search engines. This can include private discussion forums where criminals exchange information and markets where criminals sell stolen data to anonymous communication websites that restrict services like Google from indexing their contents. Deep web sites hide in plain sight, meaning that they are accessible (though sometimes only with suitable software) but are not widely promoted or discussed outside of cybercriminal circles. Deep web sites are typically exposed through tips or HUMINT collected in investigations. In any case, once cybercriminals know that their Deep web site has been exposed they may quickly pivot to another. This means the value of a Deep web site is in monitoring it for long term campaign tracking and identifying criminals (and their objectives) - and less in attempting to shut it down.

Dark Web

The dark web represents both the collection of resources available in isolated repositories, such as the anonymity network TOR[92], as well as defunct or abandoned information that is only available through archive services (such as "the Wayback Machine[93]" or Google Cache, etc.). TOR allows individuals to communicate without exposing their true location, enabling cybercriminals (as well as

[91] https://www.whois.net/

[92] https://www.torproject.org/

[93] https://archive.org/web/

users who are simply seeking privacy) to communicate privately.

Social Media

Social Media represents public communications and information sharing services. The most popular social media sites today include Facebook, YouTube, X (formerly known as "Twitter"), Instagram, and Snapchat, with many public (and private) options available. Social Media is relevant to Cybercrime as it is utilized to target victims, communicate to the public, taunt victims, provide private communications networks, and even facilitate communications with between criminal groups.

Traditional Media

Traditional Media still exists and some reporters either follow and infiltrate criminal networks or are contacted by them to facilitate objectives – such as social outcry, disinformation, or to claim accolades from their perceived "fans".

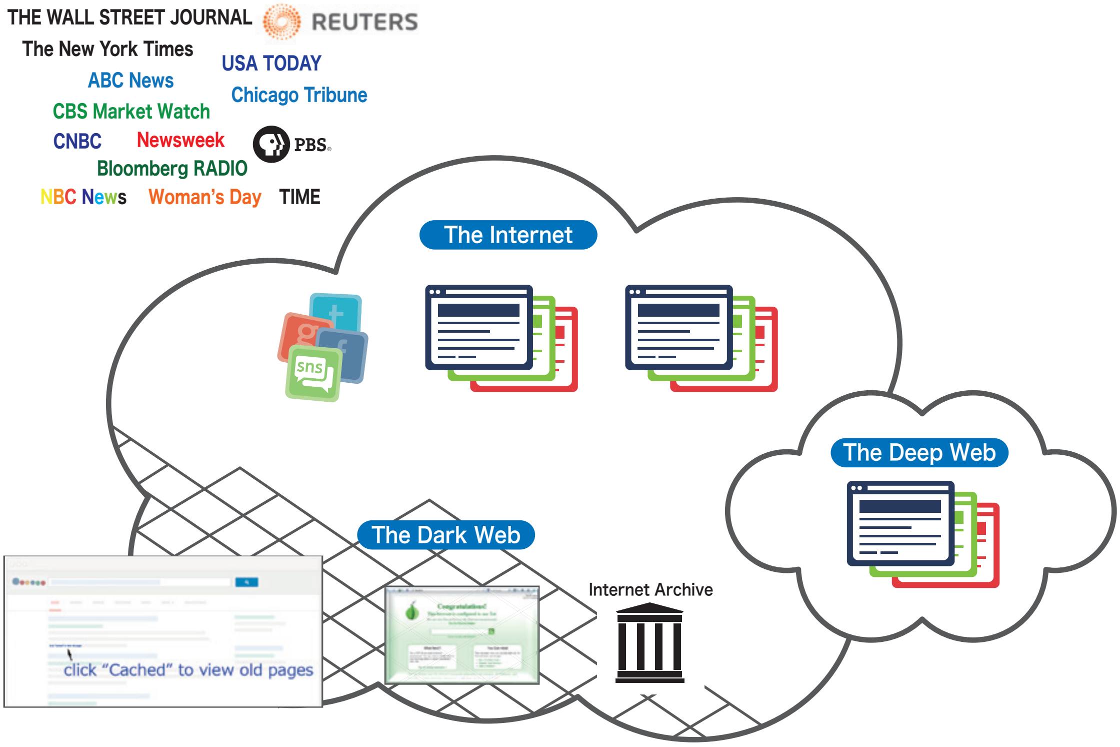


Figure 3-7. External Artifacts of Cybercrime

Criminal Networks

Most law enforcement agencies collect and develop HUMINT (Human Intelligence) either through informants, undercover officers, or purchased threat intelligence services to attempt to infiltrate criminal networks. Deep web, dark web, and other hidden communities where criminals exchange information or simply talk to other members of their own group to coordinate new campaigns are particularly valuable to investigators and intelligence collection.

Internal Artifacts

The most well understood and documented artifacts are contained in victim computers. These can be grouped into three categories of artifacts: systems, personnel and communications. Specific sources will be described in more detail in Chapter 5.

Systems

Artifacts from individual computers and applications can come from multiple sources in an *order of volatility*[94] . The higher in the order an artifact exists, the shorter its lifespan before it is destroyed through normal system operation and use.

- **Memory** – Artifacts in memory are the most volatile as any loaded program overwrites allocated memory segments. As memory is a temporary storage location, exiting files and program will release space as needed, and when a computer is shut down active memory is deleted.
- **Log files** – Depending on the operating system and related applications, log files may exist on victim systems that can provide artifacts to reveal cybercriminal actions. However, log files can be modified or deleted, and in some configurations the host system will automatically overwrite or delete log files after a period of time or according to specified storage limits.
- **Configuration settings** – Typically stored in a preference storage mechanism (in Microsoft Windows this called a registry; for macOS this is called a plist), these files store how an application was configured and may contain artifacts (such as command execution history records or services settings) that relate to stages of cybercriminal activities.
- **Operating and File System artifacts** – Specific operating and file system artifacts record user activity history. The same features developed to give the user a convenient experience when operating the computer give forensic examiners insights into past use. Some of these artifact locations store data for a period of time (internet history), some store it for a maximum number of entries (recent file accesses), and others record data until an attacker uses some kind of anti-forensics technique or tools to obfuscate their actions. These are the least volatile artifacts as they have been designed to persist in storage unless another process or user deletes them.

Personnel

Personnel can provide many different types of artifacts related to cybercrimes. The victim who first noticed an unusual behavior may provide notes for observation or interview records that assist an investigator in constructing a timeline of the crime. Staff at victim organizations can provide artifacts from evidentiary sources such as log files, physical and logical access records, and observations about anomalies in systems use and configuration. Personnel can also provide important observations and relate experiences concerning certain cybercrimes such as extortion, ransomware demands, or threatening communications.

[94] https://tools.ietf.org/html/rfc3227

Communications

Communications or network artifacts may exist in several places including billing records, configuration details of routers and switches, host configuration settings, services history logs, network traffic recordings, and systems that correlate indicators of compromise events (such as Security Information and Event Management (SIEM) logs). Many investigators neglect to consider configuration settings and billing records (as well as interviews with network security and architecture/administration personnel), but those sources can provide crucial artifacts for understanding the scope of the crime and the activities performed by cybercriminals.

Some victims may have Network Flow (netflow) data recorded as a summation of what occurred on each network connection that connects via the recording device. Most modern network devices can capture and transmit netflow data to a receiver somewhere in the victim network. Most victim organizations see netflow as a function of operations and maintenance for quality control purposes, so even if they are unaware of the threats against them, this data may exist.

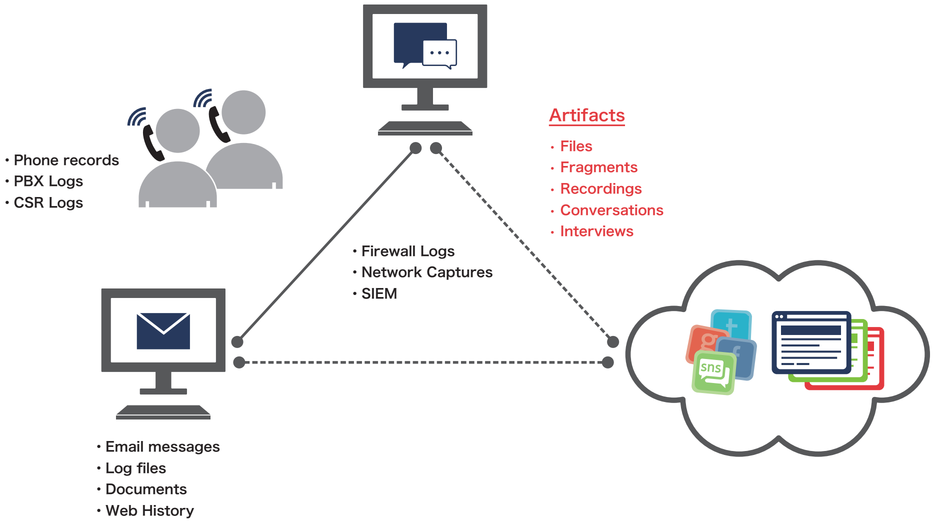


Figure 3-8. Internal Artifacts

Encryption

The exponential growth of the use of transit encryption - typically TLS, the successor to SSL - has been enabled by the ease of programmatically created certificates through services such as Let' s Encrypt[95]. Encryption is generally beneficial and offers a variety of critical benefits including end-user and transactional privacy. However, it can also be a stumbling block for network threat detection.

The use of encryption has grown significantly in the last decade, with some sources reporting growth from around 50% in 2014 to more than 90% today[96]. There has been an increase in organizations deploying TLS or SSL decryption capabilities to facilitate the decryption, security inspection, and re-encryption of user sessions. This can be complex, expensive, and difficult to achieve at scale.

[95] https://letsencrypt.org/

[96] https://transparencyreport.google.com/https/overview?hl=en

Chapter 3: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

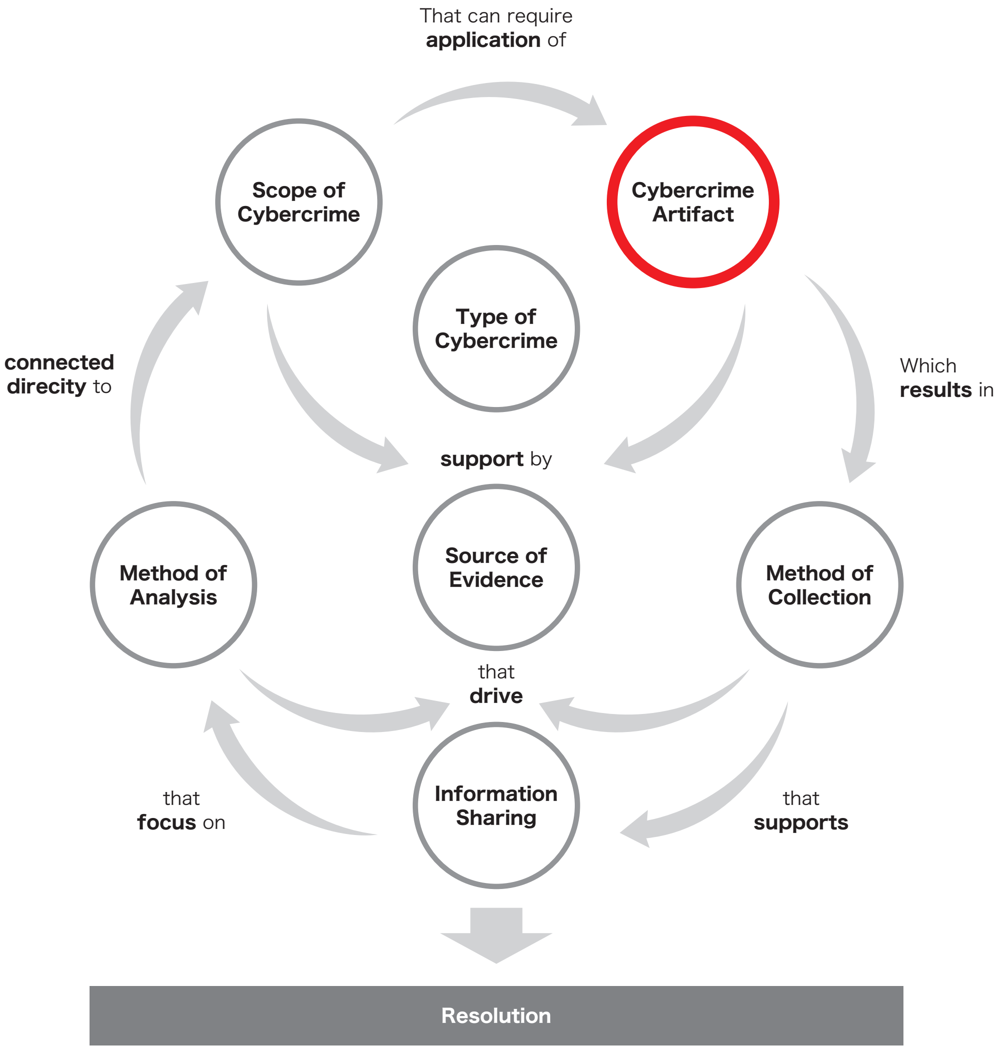


Figure 3-9. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 3-10. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 3-11. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a strategic understanding of the indicators and artifacts that will identify risks to their organization, and a tactical awareness of how to locate such information to support investigations.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence activities are tactical but require strategic awareness of indicators of cybercrimes that can assist investigators with collecting artifacts and relating to evidence of criminal activities.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. The type(s) of cybercrime will be determined by evidence according to artifacts that have been reliably discovered and analyzed.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as it relates to indicators and artifacts that may be discovered or pursued for evidence.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. Public Relations must have at least a tactical understanding of the indicators of cybercrime in order to communicate accurately the risk to the organization and its stakeholders, as well as response activities that they organization will undertake (including investigation).

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 3: Review

1. What are the indicators of cybercrime?

   Answer: Threats to the organization.

   Examples: Public disclosure of protected information, systems or services interruption, financial loss, securities performance manipulation, extortion messages.

2. How do artifacts differ from indicators of cybercrime?

   Answer: Indicators reflect the type of activity, artifacts provide details.

   Examples: Attack, reconnaissance, compromise, exploitation.

3. What are the stages of cybercrime activities?

   Answer: Related activities that are performed for varied reasons.

   Examples: Targeting, access provisioning, cataloging, service definition/administration/support/defense, service redundancy, obfuscation, alternate services, attainment of objectives.

4. What types of cybercrime artifacts are available to investigators?

   Answer: Public and proprietary.

   Examples: Log files, file fragments, communications/recordings, interviews, operating system settings, etc.

5. Where can investigators find cybercrime artifacts and indicators?

   Answer: External and internal sources.

   Examples: The Internet, the (Deep/Dark/Social) Web, HUMINT, traditional Media, Systems, Personnel, Communications.

Case Study 3: A Modern Attack

- **Crime:** Identity (credential) theft, unauthorized access
- **Suspect(s):** Iranian threat actor UNC1549
- **Means:** Social engineering, malware
- **Motive:** Political agenda (enabling potential espionage, data theft, and kinetic warfare attacks)
- **Opportunity:** Inadequate email phishing security and security awareness, political unrest

An additional layer of complexity is added to cybercrime by the fading of the lines of delineation between different types of threat groups. Historically, threat actors were split into several groups including : crimeware actors motivated by financial gain, Nation State actors seeking intelligence or the disruption of geopolitical adversaries, and Hacktivists motivated to further specific social or political objectives. Today, the boundaries between these groups are increasingly porous and blurred.

Over the past two decades, there are many examples of threat actors or groups belonging to each of these categories. This includes the Syrian Electronic Army in 2011[97] and the classic Russian Business Network (RBN) of the early 2000s[98], the plethora of recent attackers such as the Chinese Espionage Group UNC3886[99] and Nation-State adjacent APT groups[100], and modern pervasive Ransomware groups such as Blackcat, Cl0p, LockBit, and Black Basta. Long after the early signs of of "Pay-Per-Install" and the commoditization of malware distribution[101], this trend has continued unabated with widespread malware-as-a-service (or MaaS) offerings[102].

The fact that there is a human behind the keyboard must not be forgotten. Malware is just a tool, and the real threat is the human who operates it. In light of recent advances in AI, investigators must also consider the human behind an AI-enabled attack' s design, methodology, advanced tools, and machine-learning..

The true motivation a threat actor has to commit a crime is hard to determine. For example, a blue-team using its collective skills may be able to detect five compromised hosts in an environment, all of which have been implanted with binaries from a similar malware family. How confident can they be in attributing the compromises to a specific threat actor or campaign? Given the tendency for the ownership of compromised hosts to be transferred from one threat actor to another, and the commodification of cybercrime infrastructure, it is extremely difficult to understand the motivation(s) and desired outcome(s) of the specific threat actor responsible for the compromises. The risk presented by a compromised host can vary wildly depending on the responsible adversary.

[97] https://www.bugcrowd.com/glossary/syrian-electronic-army/

[98] https://en.wikipedia.org/wiki/Russian_Business_Network

[99] Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021," Mandiant, Oct. 03, 2021. Available: https://www.mandiant.com/resources/blog/chinese-vmware-exploitation-since-2021. [Accessed: Feb. 02, 2024]

[100] https://www.mandiant.com/resources/insights/apt-groups

[101] "Measuring Pay-per-Install: The commoditization of Malware Distribution" 2011, Available: https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdf

[102] https://securelist.com/malware-as-a-service-market/109980/

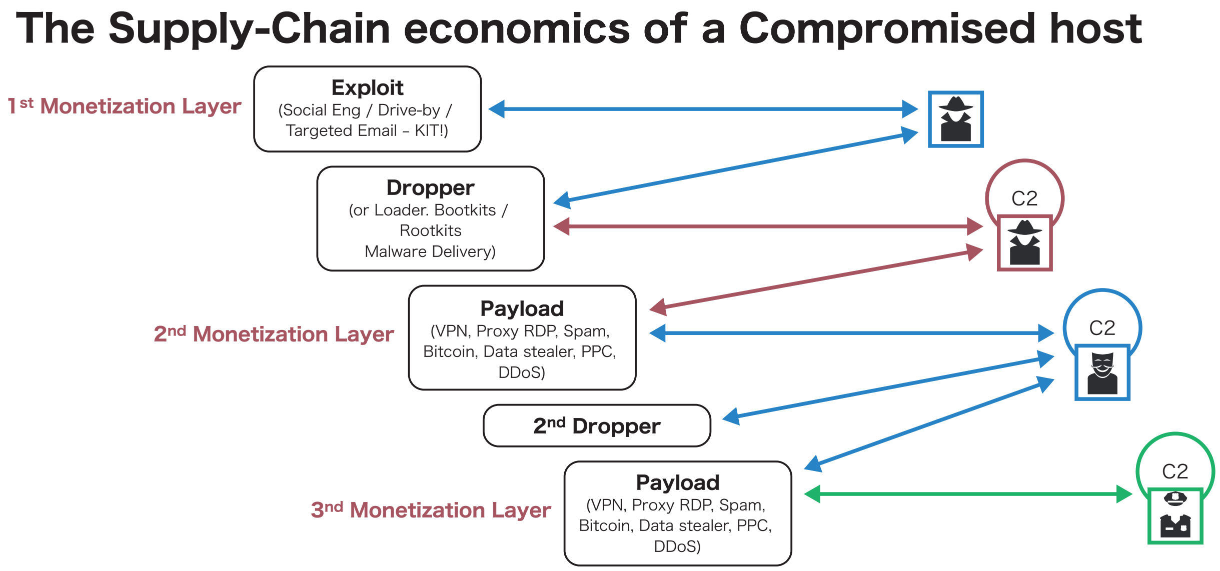

The Supply-Chain economics of a Compromised host
1st Monetization Layer
Exploit
(Social Eng / Drive-by / Targeted Email – KIT!)
Dropper
(or Loader. Bootkits / Rootkits
Malware Delivery)
C2
2nd Monetization Layer
Payload
(VPN, Proxy RDP, Spam, Bitcoin, Data stealer, PPC, DDoS)
C2
2nd Dropper
3nd Monetization Layer
Payload
(VPN, Proxy RDP, Spam, Bitcoin, Data stealer, PPC, DDoS)
C2

Figure 3-7. Supply-chain economics of a compromised host

An example of the commoditization of malware and the challenge in understanding the motivations of perceived attackers is shown in Figure 3-7 above. In this example, the targeted host is compromised by an initial exploit, after which multiple droppers (or loaders) and payloads are delivered to the endpoint. The net result is four different threat actors with access to the compromised host.

Cyber attack attribution can be incredibly complex due to a variety of factors, including the use of sophisticated techniques by attackers to disguise their identity and location like the use of "LOLbins", as previously discussed.

The following cases provide examples of cyber attacks in which initial attributions were later questioned or revised:

- Sony Pictures Hack (2014): There was initial speculation that the hack of Sony Pictures, which led to significant financial and reputational damage, was conducted by various hacker groups or disgruntled employees. Further investigation by the FBI and other entities attributed the attack to North Korea based on the tactics, techniques, and procedures (TTPs) used in the attack..

- Operation Olympic Games/Stuxnet (2010): Stuxnet was initially seen as a highly sophisticated computer worm without a clear origin which targeted supervisory control and data acquisition (SCADA) systems. It was also determined that Stuxnet was designed to damage Iran's nuclear program. It was later reported (and is now widely believed) that the United States and Israel were behind the worm. The complexity of Stuxnet and the specific targeting obscured its true nature and origin in the early stages of discovery.

- WannaCry Ransomware Attack (2017): In the immediate aftermath of the WannaCry ransomware attack which affected hundreds of thousands of computers across the globe, various theories circulated regarding potential perpetrators including criminal gangs and nation-states. Further analysis identified digital fingerprints linking the attack to the Lazarus Group- which is associated with North Korea- based on code similarities with previous malware attributed to the group.

These cases underscore the intricate detective work required in cyber attack attribution, especially when attackers skillfully utilize techniques like LOLbins to blend in with normal network activity. Such techniques not only aid attackers in achieving their objectives, but also significantly hinder investigative efforts to accurately identify attackers.

These cases also highlight the need for defined, prepared, and practiced Incident Response plans and expertise for organizations, whether through in-house or retained partner capabilities. The ability to respond quickly and effectively to an attack can minimize damage and expedite recovery.

Case study: A detailed example of a modern attack

In February 2024, Mandiant released a document detailing an attack targeting Aerospace and Defense sectors in Israel and the Middle East[103], which has subsequently been attributed to the Iranian threat actor UNC1549. The tactics used in this operation, including customized employment-themed traps and the employment of cloud services for command and control (C2), could pose significant challenges for network security teams in terms of prevention, detection, and response.

Multiple evasion techniques were used to hide criminal activity. Microsoft Azure infrastructure, social engineering schemes, and two unique and separate instances of malware- MINIBUS and MINIBIKE- were also extensively used. In addition, a custom “tunneler” called LIGHTRAIL was leveraged to further hide and obfuscate criminal behavior.

The attack lifecycle for this campaign provides a view into the complex techniques used by attackers to gain entry and implant malware tools.

1. Attackers deploy phishing attempts via email and social media messages, distributing links that lead to counterfeit websites. These websites feature content related to Israel-Hamas disputes or fraudulent employment propositions targeting technology and defense sectors including aviation, aerospace, and thermal imaging. The fraudulent job posts allow attackers to harvest credentials. In addition, clicking on the phishing links triggers the download of harmful software.

2. The infection process involves the transfer of a malicious package from the aforementioned sites directly to the victim's device. The package is an archive containing two primary components:

   - MINIBIKE or MINIBUS: Distinct types of malware capable of providing comprehensive unauthorized access to the infected system. MINIBIKE first appeared around 2022 and MINIBUS appeared around 2023. Both enable data exfiltration and uploads, in addition to command execution

   - Either a decoy application designed to appear as the legitimate application OneDrive (in the case of MINIBIKE) or a bespoke app displaying information about Israelis held by Hamas (in the case of MINIBUS). The MINIBUS application also directs users to the fraudulent site birngthemhomenow[.]co[.]il.

[103] https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

An extensive list of the IoCs and IoAs employed during this attack is outlined by Mandiant. Notably, file hashes, registry keys and values, specific browser User-Agents, persistence mechanisms, dedicated C2 infrastructure, and C2 URLs are seen, all of which differ across subsequent versions of the tooling used in the attack. This highlights the complexity and breadth of techniques used to perpetrate a nation-state attack.

Chapter 4

Scope of Cybercrime

Introduction

A person is shot. That may or not be a crime depending upon the circumstances. The person is intentionally shot. It may still not be a crime. The person is not shot in a war, but in a community area. The circumstances are still unclear. The person is intentionally shot in a crowd attending a social demonstration. Perhaps the shooter had a legitimate reason such as self-defense? The person who was shot was speaking to the crowd attending the social demonstration. There may be a crime here. The person who was shot was Martin Luther King.

Any crime is defined by the actions, intent, and impact that relate to the act. The nature of the crime is defined by the same criteria; the differentiator is fundamentally the "scope" of the crime. A crime such as described above is different if the person who was shot was a soldier in a war, or even a bystander to a demonstration, versus MLK. This is simply because the impact of the criminal act has a broader scope. The threat, or consequences if the crime has already been committed, differ according to the objective(s) and the methods of achieving them.

Another scenario may be useful to describe more common cybercrimes. A security system alerts a service that a building has been accessed without appropriate codes. Police respond and discover an open door. Further examination shows a broken pane of glass that allowed the door to be opened from within. Police discover a homeless person sleeping just inside the building.

The same scenario, but this time police also notice lights on in an office down the hall from the homeless person. A computer is turned on (odd because all others are off), and a folder on the computer desktop is opened to a file called "Mergers 2016" with a "Copy Complete" dialog box on the screen. Upon questioning, police learn from the homeless person that the door was already open when he came in from the cold for a safe place to sleep.

As sensational as these crimes sound, they are unfortunately representative of types of crimes facilitated by cyber tools, tactics, and procedures (TTP' s). Murder, societal subversion, trespass, intellectual property theft, and extortion are all types of crimes facilitated by cyber – but their impact is ultimately a deciding factor according to the scope of the crime in its commission and results.

A random computer infection that results in an attempted botnet subscription to a service that is no longer available differs entirely from a targeted computer infection that spreads to corporate computers to enlist botnet drones that enable a cybercriminal to steal information, eavesdrop upon corporate performance data, and sell access to corporate systems – to subscribers of their botnet. A computer intrusion to enlist a computer into a botnet also differs from a rogue trader who subscribes to a botnet for purposes of insider trading with non-public information they gain access to thereby.

Since 2013, the scope of cybercrime has expanded significantly, with evolving motivations and lowering levels of technical skills required to conduct attacks driving an increase in criminal activities. The motivation to conduct a cyber enabled crime remains primarily financial in nature. However, the ability to use technical applications to conduct sophisticated crimes of intellectual property, non-public market information, and state secret thefts along with motivations of sabotage, ideology, orders, ego, and hatred have all grown accordingly. Moreover, with the significant market growth and broader adoption of cryptocurrencies by financial services, ransomware has evolved into the preferred toolset for criminal and nation-state supported actors looking to further their broader objectives. The following examples illustrate the changing landscape of cybercrime between 2013-2024, and looking forward:

1. **Financial Gain:** The primary motivation for cybercrime remains financial profit, with fraud and theft as the primary objectives. Hackers use various methods such as credential replay, phishing, social engineering, and the online recruitment of insiders to collect, sell, or use for themselves credit card details, online retail, bank account, cryptocurrency wallet, and gaming logins, and associated personal identifiable information (PII) for financial gain[104]. Financial crimes beyond simple frauds, swindles, and scams of individuals by way of online account takeovers have evolved into sophisticated financial criminal activity including insider trading, wire fraud (i.e., Business Email Compromise), mobile banking deposit fraud, and direct cryptocurrency thievery.[105]
2. **Ideology/Orders:** Some cybercriminals are motivated by ideology[106], which can make them a more challenging threat and create difficulty in assessing the scope of the crime. The ideology is increasingly motivated by political, environmental, or religious radicalization and can be fueled by a variety of psychological disorders. Nation-state sponsored attacks (including acts of war, i.e. critical infrastructure sabotage) and organized or decentralized criminal gang hacking activities have increased alongside cases in which hackers follow direct orders due to their employment within a military unit or intelligence agency, indicating a growth in ideological principles and radicalization alongside professional motivations behind cybercrimes[107] [108]. For example, the significant investment by companies and nation-states in the research and development of intellectual property, particularly in technology (quantum computing, Artificial Intelligence (AI), robotics, blockchain, etc.), transportation, medical, defense, and space capabilities, has increasingly motivated the theft of data by state-sponsored and criminal actors hired to conduct business-to-business attacks which facilitate various competitive, financial, and national security objectives.
3. **Compromise:** Insider threats and compromised employees can also be motivating factors in cyber-attacks. Differences in opinions or personal gain may lead employees to compromise their organizations' security[109].
4. **Ego:** The desire for recognition and achievement also motivates cybercriminals. Some hackers seek to boost their reputation by successfully compromising major systems, driving each other to complete more complicated hacks[110]. With the significant growth in bug bounty programs, it can be difficult to determine if only ego motivated a hacker to conduct an attack or if they were also financially motivated with hopes the victim would pay them to not publicize the vulnerability and/or system compromise.
5. **Hatred:** Cybercrimes against individuals, such as cyberstalking, cyberbullying, impersonation, sextortion, and revenge pornography, are often motivated by hatred and the desire to inflict pain and harm[111]. The growth in these types of cybercrimes is also directly associated with the explosion of social media use and platform, hardware, and software enhancements (e.g., cellphones, cameras, video editing, deep fakes, etc.).

[104] https://www.coretech.us/blog/6-motivations-of-cyber-criminals
[105] https://www.fraud-magazine.com/article.aspx?id=4295019793
[106] https://www.sophos.com/en-us/cybersecurity-explained/threat-actors
[107] https://stratixsystems.com/what-are-the-motivations-for-cyber-attacks/
[108] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[109] https://stratixsystems.com/what-are-the-motivations-for-cyber-attacks/
[110] https://www.coretech.us/blog/6-motivations-of-cyber-criminals
[111] https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

The scope of cybercrime has changed significantly in the period 2013-2024, with an increase in the rate of attacks, the number of records stolen from breaches, and the financial impact. The evolving motivations behind cybercrime have led to a more complex and challenging threat landscape, requiring continuous adaptation and improvement in cybersecurity measures. The opportunities to exploit technology to achieve financial and economic competitive benefit have proven irresistible as well, with insider-supported cybercrimes becoming common[112] and supply chains representing vast weaknesses to organizational security[113].

Cybercriminals, in particular ransomware groups and their affiliate members, are growing more emboldened each day given the ease with which they can carry off attacks and growing challenges for enforcement officials seeking to ensnare and hold accountable all participants and conspirators. The lack of deterrence is leading groups to attack segments of critical infrastructure and commerce. In 2024 alone, attacks on bank trading systems, major healthcare provider payment systems, and state and local governments have been observed among others. The size, scale, and scope of attacks is continuing to grow, making it more difficult to manage the economic devastation which occurs.

At the same time, the cybersecurity industry is experiencing rapid growth, with an increasing number of job openings and a shortage of skilled professionals. The global priority placed on cybersecurity reflects the growing frequency and impact of cybercrime, making it essential for businesses, organizations, and the public to embrace cybersecurity[114].

The estimated global cost of cybercrime is expected to reach $10.5 trillion annually by 2025, representing a significant transfer of economic wealth and posing a substantial risk to innovation and investment[115]. The changing landscape of cybercrime highlights the need for robust cybersecurity measures, increased awareness, and a skilled workforce to combat the growing threats effectively. In addition, there is a need for investigators to consider all aspects of cybercrime to fully understand, investigate, and resolve the entire scope of the criminal act by not just focusing on the “cyber” technical details without considering the “crime” being committed.

This chapter will explore the concept of “scope” in understanding and assessing cybercrime. The nature of the crime, its purposes of targeting (to achieve designed objectives that the TTP’ s facilitate), and differences between public and private organizations will be described. This chapter will help an organization define governance criteria for directing investigations and developing associated policies, systems, and procedures for defense and protection.

At the conclusion of this chapter, readers will have understanding of:

- What are the different “natures” of cybercrimes?
- What organizational functions do cybercrimes target?
- How have insiders and supply chains expanded the threat and impact of cybercrimes?
- How do risks to those functions differ in public versus private organizations?

[112] https://www.code42.com/blog/insider-threat-examples-in-real-life/

[113] https://www.bluevoyant.com/knowledge-center/supply-chain-attacks-7-examples-and-4-defensive-strategies

[114] https://ung.edu/continuing-education/news-and-media/cybersecurity.php

[115] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Topic in Scope of Cybercrime

Figure 4-1 displays topic categories in the “Scope of Cybercrime” knowledge domain.

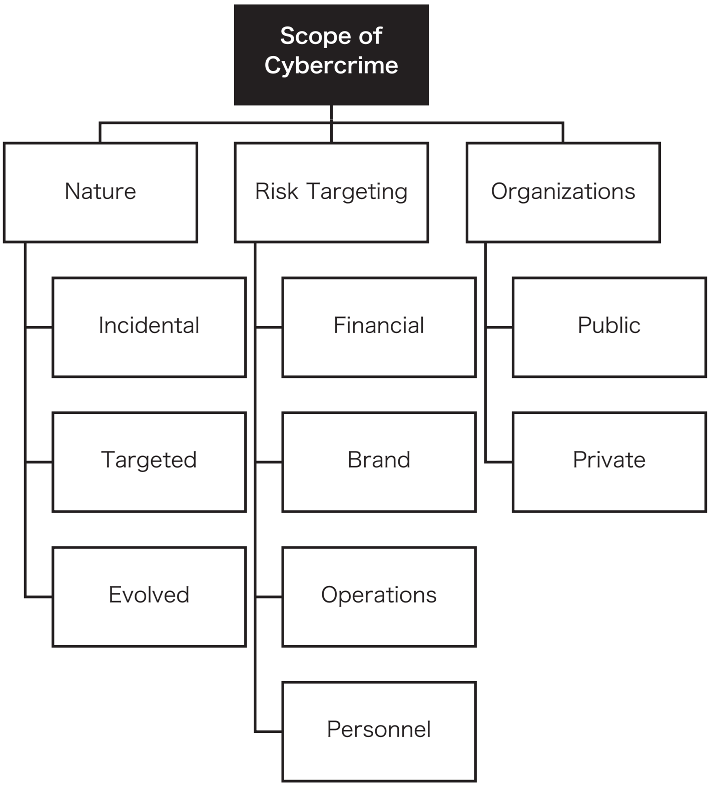


Figure 4-1. Topic Categories in the “Scope of Cybercrimes” knowledge domain

What is the Scope of Cybercrime?

The scope of cybercrime refers to both the scale of cybercrime organizations, as well as the scope of victims or their associated computers. Cybercrimes differ in nature and according to the organizational or personal risks they exploit. The scope of victims therefore differs. For example, third-party botnet developers (who use spam to phish and waterholing techniques to hook victims) are usually small or independent operators of virtual platforms, so the scale of their organization is small – but the scope of their victims is sometimes very large if their intent is incidental (drive-by) compromise. Other entities who make use of the access that the botnet developers offer can conversely have large established organizations with developers, administrators, and even skilled business functional staff to exploit targeted objectives of victim organizations' resources – such as financial systems and processes. In that case, the scope of the victim is small but the risk is potentially higher. As previously discussed in Chapters 2 & 3, the types and artifacts of cybercrimes can be complex, but ultimately the determination of the scope (for impact analysis) of a cybercrime depends upon the objective crime(s) committed and who benefits.

Investigators often overlook the issue of scope when assessing attacks or compromise of victim computers and networks. Focusing upon discreet indicators of compromise leads to myopia (tunnel-vision) and a misunderstanding of the crime(s) that otherwise may be evident from an assessment that considers the entire IT estate, including partner and vendor networks when interconnected. Sources of evidence and methods of collecting and analyzing evidence at the scale of the organization that will enable an investigator to determine the scope of cybercrime(s) will be addressed in Chapters 5-7.

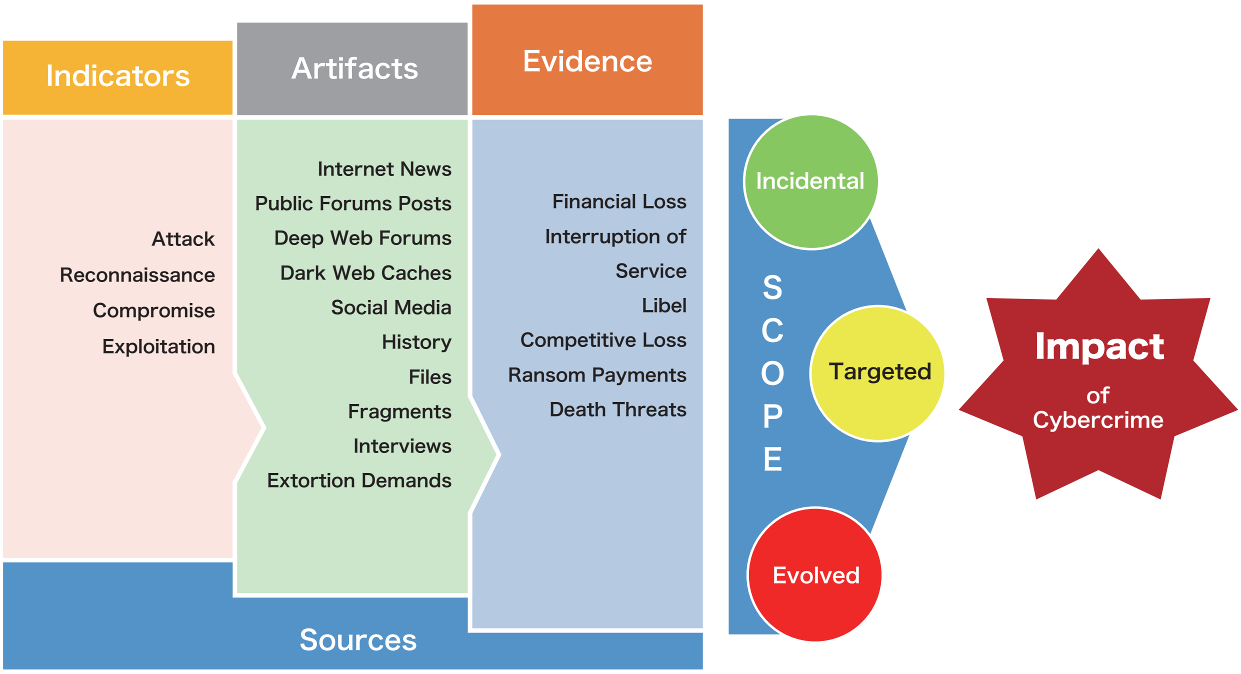


Figure 4-2. Scope of Cybercrime

The digital age that has come about due to the growth of technology, the reliance and emphasis individuals and organizations place on it to increase everyday life and workplace efficiency, and the continuous race to invent new or improved applications and devices has flattened the world. Millions of people across the globe harness the convenience and power of technology. This is most often through Internet connectivity to support their varied needs to communicate, entertain, shop, educate, bank, heal, and create. The human condition has unquestionably advanced, and the interconnected world has ushered in prosperity and opportunity.

Most technological advancements (in this case the Internet) that have improved the human condition often provide opportunities to exploit/harness the same for nefarious purposes. The expansion of the virtual world has brought with it the opportunity to commit crimes where historically the existence of the physical world of buildings, guards, borders, waterways, as well as traditional law enforcement practices of physical evidence collection and jurisdictional commonalities have worked to combat and contain transnational crimes[116]. This new way of committing the same types of crimes of fraud, theft, espionage, and extortion, has grown in size, scale, and scope; and it is simply explained as being the "transformation of criminal or harmful behavior by networked technology"[117].

The billions of records stolen from data breaches have fueled a growth in the number of people who can participate in cybercrime, leading to a significant expansion in the size of organized and disorganized cybercriminal groups. Recent events have shown that some financially-motivated cybercriminal activities are carried out by groups with distinct divisions of labor. Those divisions include networks of people who are recruited—often referred to as mules—who although unrelated to cyber activities, are necessary to accomplish the last part of a financially motivated cybercrime. That cycle of activities includes placing, layering, and integrating (i.e. money laundering) their stolen funds into bank accounts that are usually located in countries uncooperative with Western law enforcement.

In a 2010 statement, the Federal Bureau Investigation (FBI) highlighted the following functions of a well-organized criminal fraud conspiracy to describe how the business of cybercrime has grown[118]:

- "Coders or programmers write the malware, exploits, and other tools necessary to commit the crime.
- Distributors or vendors trade and sell stolen data, and vouch for the goods provided by the other specialties.
- Technicians maintain the criminal infrastructure and supporting technologies, such as servers, ISPs (Internet Service Providers), and encryption.
- Hackers search for exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access.
- Fraud specialists develop and employ social engineering schemes, including phishing, executive "whaling", spamming, and domain squatting.
- Hosts provide "safe" facilities of illicit content servers and sites, often through elaborate botnet and proxy networks.
- Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers or 'money mules'.

[116] Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Doubleday.

[117] Tabansky, L. (2012). Cybercrime: A National Security Issue? Military and Strategic Affairs, 4(3), 117-136.

[118] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An Analysis of the Nature of Groups Engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

- Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location.
- Tellers assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies.
- Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds"

The scale of operation in organized cybercrime groups is evident in the described roles and responsibilities of the staff involved. The creation of reusable tools and infrastructure also infers the scope of victims intended to be targeted and exploited (to achieve their goals of financial theft and fraud). A diagram of how a cyber theft (/fraud) ring operates[119] is provided in the following figure.

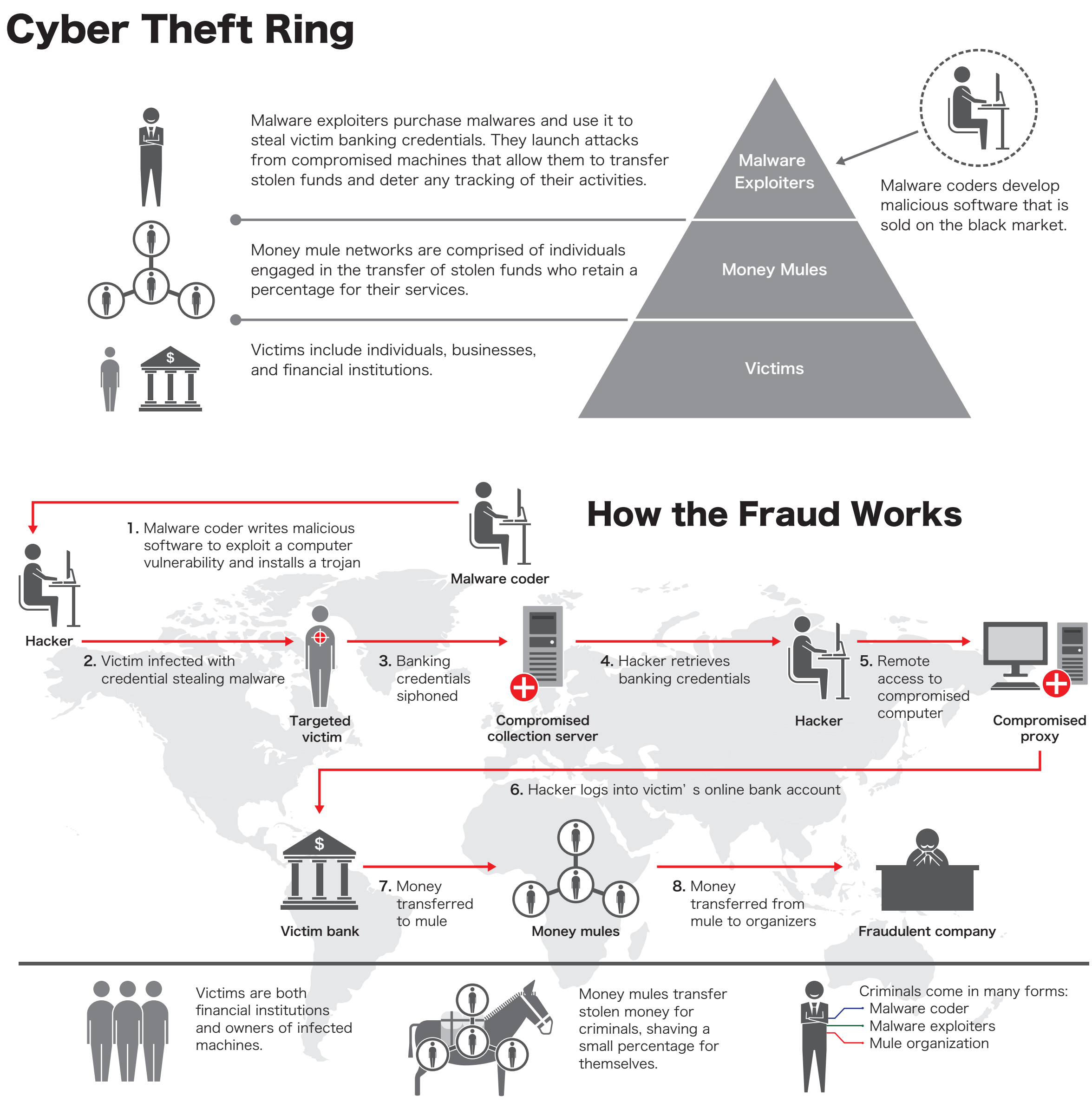

Cyber Theft Ring
Malware exploiters purchase malwares and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.
Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.
Victims include individuals, businesses, and financial institutions.
Malware Exploiters
Money Mules
Victims
Malware coders develop malicious software that is sold on the black market.
How the Fraud Works
1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan
Malware coder
Hacker
2. Victim infected with credential stealing malware
Targeted victim
3. Banking credentials siphoned
Compromised collection server
4. Hacker retrieves banking credentials
Hacker
5. Remote access to compromised computer
Compromised proxy
6. Hacker logs into victim' s online bank account
Victim bank
7. Money transferred to mule
Money mules
8. Money transferred from mule to organizers
Fraudulent company
Victims are both financial institutions and owners of infected machines.
Money mules transfer stolen money for criminals, shaving a small percentage for themselves.
Criminals come in many forms:
Malware coder
Malware exploiters
Mule organization

Figure 4-3. Cyber Theft Ring

[119] https://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-scam.htmlgraphic

It is unclear how many well-organized cyber fraud crime rings exist and operate under the structured model reminiscent of “mafia” crime families. Identifying and bringing to justice the individuals responsible for the large financially-motivated events or the massive data breach intrusions such as the 2015 U.S. Office of Personnel Management (OPM)[120], that dominate the news headlines, are proving to be elusive and daunting tasks for law enforcement. Two cybercrime events, the theft from Bank of Bangladesh through the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system[121] and the stock traders who pled guilty to executing securities transactions based on inside information stolen by hackers[122] emphasize the point that cybercrime has evolved not from the perspective that the cyber tools being utilized have become more exotic, but that the types of systems serving commerce (e.g. SWIFT) and market activities are being exploited to commit crimes like fraud and theft. This has enabled cybercrimes to grow in scale, and the scope of cybercrime to involve not only the direct victims but also indirect victims.

It also highlights the following important points:

- The hackers are not necessarily the same people who are actually executing and responsible for the subsequent criminal objectives.
- The opportunities and ability to commit highly-lucrative crimes have evolved.
- The level of business functional knowledge needed to carry out the crimes reveals the extent to which other skill-sets are being employed.
- Law enforcement and related investigations should focus attention on the objective crimes according to the nature and scope of the crime, and not interpret the tools or incidental activities out of context to the objective(s).

Most people think cybercrime actors only equate to those who have the ability to create malicious software. While it is true these actors do make up some portion of the total participants in the cybercrime ecosystem, cybercriminals have capitalized on their commodity of knowing how to develop malicious tools by making them available for purchase on the portion of the Internet that is not available through popular search engines such as Google and Bing. This portion of the Internet, which is larger than the indexed portion everyday people access, is known as the Deep and Dark web.

The Deep and Dark web, also referred to as the “Darknet,” were previously described in Chapter 3. The Darknet is full of numerous “E-Bay” like marketplaces that put up for sale malicious tools like exploit kits, malware, compromised network infrastructure (e.g. servers and computers), and rights to access databases which contain stolen banking credentials, credit card numbers, personally identifying information (PII), and sensitive business information concerning ongoing mergers and acquisitions. These items are obtained from other illegal activities such as the intrusions into healthcare and insurance providers like Anthem BlueCross[123], law firms[124], and retail providers like Home Depot[125].

[120] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[121] http://www.reuters.com/investigates/special-report/cyber-heist-federal/

[122] http://fortune.com/2015/12/21/trader-pleads-guilty-in-insider-trading-hacking-case/

[123] http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

[124] http://fortune.com/2016/04/04/panama-papers-law-firm/

[125] http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

It is clear that hacking is no longer just an event. It is a process that begins with the application of myriad methods and tools to assist the hacker with gaining access to a network or data source. Malware, phishing, ransomware, and other approaches are employed with targeted or opportunistic intent. After the intrusion, the stolen data is advertised on social media, open web dumpsites, Darknet marketplaces, and other mediums where it is packaged and repackaged for sale. Notably, these criminal business transactions can take place weeks, months, or even years after the original network compromise. An explanation of dark web marketplace dynamics reveals the complexity which investigators must account for in order to properly define the scope of cybercrime.

Hackers steal information for financial gain or for the future procurement of other more valuable information. Like any successful business model, money is exchanged for goods (in this case, stolen data) at a market rate based on supply and demand. The demand for stolen data has grown exponentially because of its high margin of profitability and relatively low risk of law enforcement action. However, the stolen information, compromised computer, or system access being sold must be usable and valid for the secondary criminal to receive a return on their investments. Similarly, a hacker' s reputation for supplying usable and valid data is imperative to the hacker' s own return on investment. Even nation-state hackers seek usable and valid information from well-regarded cybercriminals. Reputation is the bread and butter of the cybercriminal industry, so hackers are careful to manage the quality and validity of stolen data.

After employing means to accumulate stolen data for distribution, the best hackers test the validity of the information using methods typically undetected by cybersecurity protocols (e.g., a quick email login, an account balance check, a small charge on a payment card, etc.). Validating data takes time, but once authenticated the data can be packaged and repackaged for different criminal uses (fraud, insider trading, espionage, etc.). Finally, hackers offer the data for sale on Internet marketplaces and other mediums. In this lapse of time between the initial hack and the future use of the hacked information, a gap exists in the hacker-criminal business engagement. This gap continues to grow as hackers increasingly specialize in the varieties of data they sell to an increasingly discerning criminal marketplace and thus continues to expand the scale and scope of cybercrime.

A booming criminal economy of willing buyers, sellers, and resellers of data and access is fueled by hackers stealing data with various methods and objectives. This includes hackers running phishing campaigns, those facilitating first stage botnet malware access for ransomware gangs who utilize second stage malware to encrypt systems and steal data, those breaching systems and exfiltrating data, and those operating toolsets to persistently scan and scrape social media sites to enable the creation of targeting packages for nation state actors. It is the buyers who utilize the stolen information and/or compromised computer or network access to conduct follow-on criminal acts such as fraud, theft, and espionage that accounts for the record growth in victims and financial damage since 2013.

The expansion of criminal subscription marketplaces, also known in the cyber community as Cybercrime as a Service (CaaS)[126], has expanded at a rapid pace since the investigation into the individuals responsible for a forum called Silk Road became public[127]. The Cybercrime as a Service (CaaS) model has expanded and cybercriminal organizations have matured their business models

[126] http://resources.infosecinstitute.com/cybercrime-as-a-service/

[127] https://www.rt.com/usa/silk-road-bitcoin-shut-650/

with all of the needed functions (e.g., call centers, payment protocols, etc.) and processes of a legitimate business. CaaS organizations hire hackers and incentivize them like employees of normal organizations, employ call center representatives to service customers, and create defined layers of management and structure, revenue goals, and organizational objectives. The business of CaaS has evolved into industry unto itself.

The largest growth area in the CaaS model involves ransomware. Most if not all groups creating encryption malware lease out their toolsets to affiliate members who are tasked with gaining network access to then steal data and deploy payloads. Victims are then provided a cryptocurrency address to pay ransoms that are split with the group which created the malicious software. Organizing criminal activity in this revenue sharing model creates business continuity for criminals, making it harder for officials to pursue all responsible parties. A less sensational and not as well-publicized demonstration of the CaaS model is observed daily at U.S. banks. The cybercrime is perpetrated by U.S. based street gangs who subsequently use the proceeds of bank fraud to commit other criminal acts. The scheme to defraud works as follows:

> The remote deposit capture feature on cell phone banking applications is used to place fraudulent checks into a bank account of a willing participant who has been recruited through social media. Gang members collaborate through Meta, formerly known as Facebook, with mostly Nigerian cybercriminals to purchase and deposit fake checks created with data obtained from previous data breaches. The checks are usually purchased using cryptocurrency. Upon the deposit of the fake checks, gangs stage members close to Automatic Teller Machines (ATMs) in multiple locations to withdraw all funds in the account before the check is declined for being fraudulent. The participant who allowed their account to be utilized for the fraud subsequently files a complaint with the bank claiming to have suffered an online account takeover. In many instances, banks return funds of the original balance before the deposit of the fake check.

Although the CaaS economy is another challenge for law enforcement to combat, it does create a unique opportunity to establish an anonymized presence as a basis for intelligence collection, deploy online undercover operations, and most importantly to identify opportunities to spot, assess, and recruit the type of intelligence needed to contextualize and provide meaning to the electronic intelligence (ELINT) events - Human Intelligence (HUMINT). These types and efforts of intelligence support investigators by helping to assess and develop awareness of objectives, scale of cybercrime organizations, and scope of victims.

The following graphics provide an overview of the types of information, services, products and actors that can be found operating within the Darknet[128].

[128] https://www.linkedin.com/pulse/darknet-deep-web-explained-bradley-w-deacon, originally found at http:// http://www.batblue.com/the-darknet/

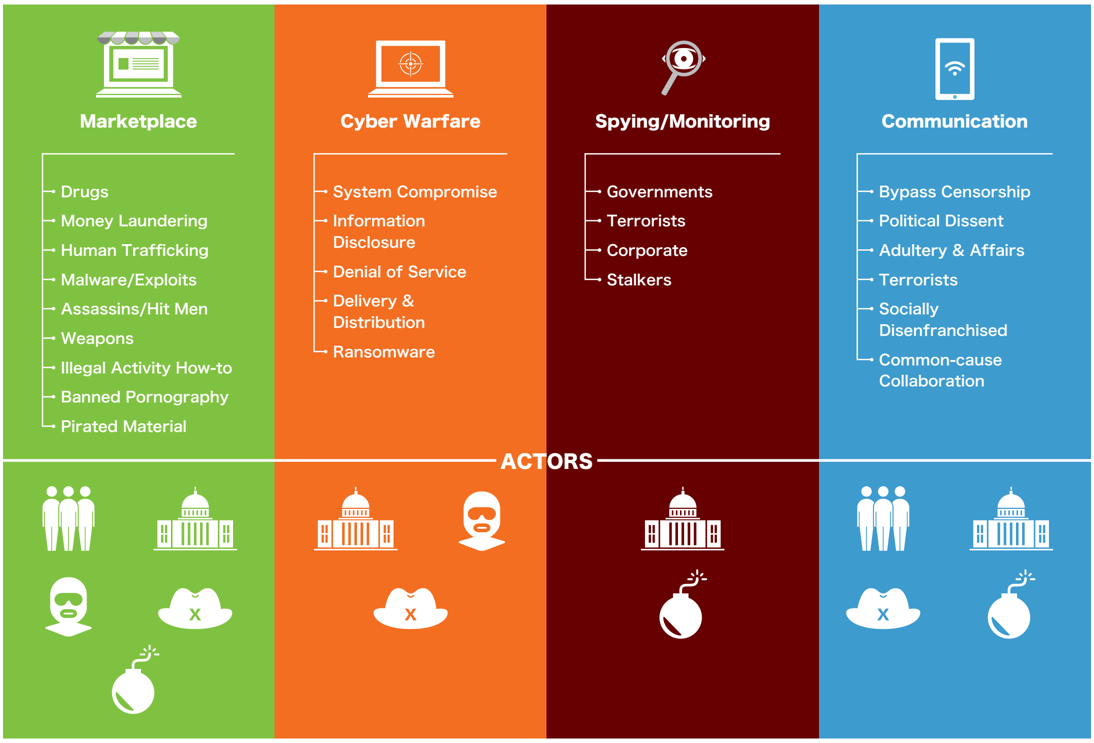


Figure 4-4. Darknet Offerings

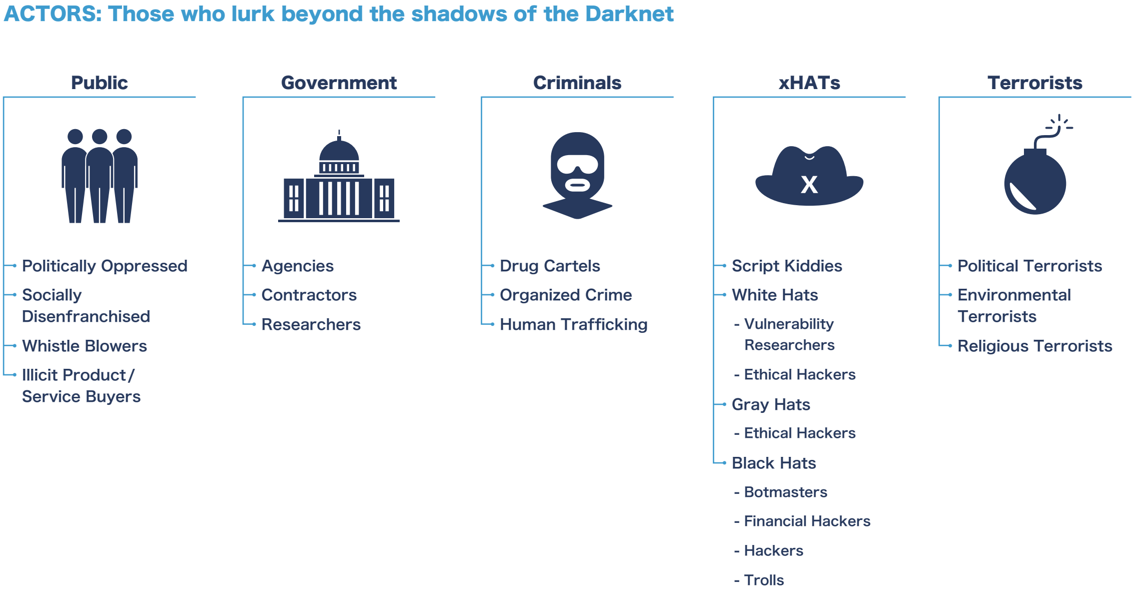


Figure 4-5. Darknet Profiles

The online world has eased the ability to commit—often with impunity—crimes of convenience (e.g. theft), opportunity (e.g. fraud), and purpose (e.g. sabotage) because of the ease in which individuals and/or groups can exist, operate, disassociate, and hide across world-wide jurisdictional lines. The scale of economic damages is facilitated by the increasing ability to conceal connections to criminal activities. This is because of inventions such as cryptocurrencies (e.g. Bitcoin) and their integral role in the previously discussed virtual underground marketplaces in the Darknet. The opportunities for cybercriminals to leverage computing skills for multiple purposes is challenging even for the most sophisticated law enforcement agencies.

This confusion has been seized upon by sophisticated criminals who blend resources, use malicious software tools, share (inter)network infrastructure, utilize shell companies, and manage bank accounts under fake (or stolen) identities to carry off crimes that force law enforcement organizations to spend significant amounts of time trying to determine if and how the crime should be investigated. The "how" is subject to complex jurisdictional issues as discussed in Chapter 1, and sometimes it is hampered by procedures that have not kept pace with the evolution of technology and related cybercrimes.

The evolving role and use of digital assets, particularly cryptocurrencies, must be discussed in depth to fully understand the complexity of cybercrimes today. Cryptocurrencies have become widely adopted by consumers and financial institutions – including broader adoption in capital markets with the recent U.S. Securities and Exchange Commission (SEC) approval of Bitcoin (BTC) Exchange-Traded Funds. According to CipherTrace, a Mastercard Company, "the cryptocurrency market cap went from approximately $135 billion on January 1, 2019, to just under $2.1 trillion on March 31, 2022, which is an increase of 1,456 percent. That cryptocurrency market cap peaked in November 2021 at almost $3 trillion, at which time Bitcoin hit its all-time-high of $68,790." [129] Since the reporting by Ciphertrace, Bitcoin recently crossed the $70,000 threshold setting a new all-time market cap record.

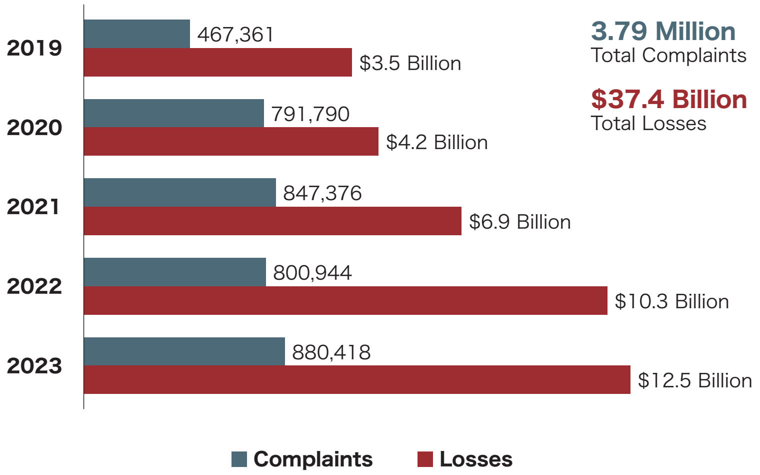
At the same time the crypto market has expanded, there has been a rapid increase in insider trading, fraud, bankruptcy proceedings across industries and significant adoption by cybercriminals, terrorist groups, and transnational organized crime. Cryptocurrencies have become integral to many if not most cybercriminal operations. The degree of anonymity offered by these currencies makes it difficult for law enforcement agencies to trace transactions back to individuals and exchangers facilitating clearing accounts for fiat conversion. This has facilitated the growth in ransomware attacks among other crimes, as cryptocurrencies are now commonly used on the Darknet for illicit activities such as drug trafficking, weapons sales, and the sale of hacking tools. The decentralized nature of cryptocurrencies allows these transactions to occur beyond the reach of traditional law enforcement.

As digital assets and cryptocurrencies continue to be adopted rapidly across industries and ecosystems, the integration of digital forensics and analytics to help identify and report on key findings becomes increasingly essential. The ability to navigate the complexities of blockchain transactions, trace ownership, and attribution to individuals is critical to investigating events related to fraud, theft, extortion, scams, and other illicit activities. Overall, while cryptocurrencies offer numerous benefits, their decentralized and pseudonymous nature also presents challenges for law enforcement in combating cybercrimes. As the popularity and adoption of cryptocurrencies continue to grow, it's likely that cybercriminals will continue to exploit them for illicit purposes, further expanding the scope of cybercrime.

Unless investigators and intelligence agencies can comprehend the scale of cybercrime organizations, the scope of victims associated with the crimes they commit will not be understood. Evidence supporting the growing scope of cybercrime is found in the Federal Bureau of Investigation' s (FBI) most recent annual Internet Crime Complaint Center (IC3) report from 2023[130]. The following charts taken from the report summarize the number of complaints and losses from 2019 until 2023, the impacts of various types of cybercrime 2023, and the impact to victims by age group.

[129] Cryptocurrency Crime and Anti-Money Laundering, CipherTrace, Mastercard, June 2022 Report

[130] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf



quickly evolved

Nature of Cybercrime

Too much attention and focus during cybercrime investigations has been placed on identifying and neutralizing the network infrastructure [i.e. servers, Internet Protocol (IP) addresses, website domains, etc.] utilized by cyber actors and investigating how malware functions or operates (i.e. reverse engineering). These investigative activities are important, but only from the perspective of determining the scale and scope of the activities. These activities should be performed by analysts supporting the investigation. The information derived from these activities should be utilized as a data point or listed as a fact of the investigation, rather than functioning as the basis for conducting (or interpreting the results of) an investigation.

Most cybercrime investigations are initiated after a public announcement, organizational self-reporting, or law enforcement notification. Information could also be derived from a variety of sources (to be discussed in Chapter 5) including but not limited to human intelligence (HUMINT), Signals Intelligence (SIGINT), or published research. Some investigations are initiated in response to alerts generated by an organization’ s security monitoring tools. During the initial victim engagement process with either a public or private organization, it is extremely important—and largely only possible with a cooperative victim—to attempt to gain detailed answers to the following list of questions (not all-encompassing), which will assist in developing an investigative theory and approach:

1. Who in the organization was targeted and when?
2. What type of systems were targeted?
3. What business functions do the systems serve?
4. Were sensitive data or applications compromised and if so, what is the risk?
5. How were the targeted systems then used? For example, were the systems used as a pivot point for other system access? And if so, see the questions above.
6. What risks concern you the most about this incident—protected non-public information loss, brand/reputation degradation, financial loss, business interruption, lawsuit, etc.?
7. Has there been any contact from purported attackers? If so, what are their requests?

8. Who is the point of contact I need to engage to provide the necessary legal processing (subpoena, national security letter, or consent form) for purposes of evidence collection?

The approach should largely mirror how investigations into crimes of fraud, theft, money laundering, espionage, etc. have been conducted historically. Defining the scope by the nature of the cybercrime becomes critically important in order to avoid wasting time and resources on procedures largely unnecessary to proving who committed the crime - or more importantly, why they committed it. If the investigative team can properly identify the true nature of the crime, which is often not simply the unauthorized access and use of a system, a more meaningful enforcement mechanism will be achieved because punishment, especially under U.S. law, is much harsher for crimes such as wire fraud and money laundering than unauthorized access or CFAA violations[131].

It has become even more crucial during a cybercrime investigation to ask the types of questions listed above as even well-known commodity malware has evolved to facilitate complex cybercrimes. Any computer that has been compromised and added to a network of other compromised computers (often via installed malware) – belongs to a "botnet", even in notorious APT activities that leverage custom malware. A bot is " 'a type of malware that an attacker can use to control an infected computer or mobile device. A group or network of machines that have been co-opted this way and are under the control of the same attacker is known a 'botnet'" [132]. Botnets facilitate automation tasks and can be used for multiple types of cybercrimes including DDoS and e-mail spam for spear phishing campaigns. They can be used by multiple independent or affiliated cybercriminals – anyone can create a botnet thanks to the availability of commodity tools, and anyone can operate a botnet thanks to the availability of commodity services.

Many types of malware exist, but a significant number have been derived from the "grandfather of botnet malware" called "Zeus". Zeus malware was publicly released for free use and development on the Internet in 2011[133], though it was available for purchase on many Darknet forums previously. Perhaps not coincidentally, botnets have since exploded in scale around the world and derivative versions of popular botnet malware (paid-for and free) are constantly being released. As noted previously, CaaS services have grown with the availability of supporting infrastructure and interested cybercriminals. These services have evolved to incorporate subscriber access for managed access and use of compromised computers. In an article titled *A Dummies Guide to 'Insider Trading' via Botnet*[134], a historical evolution of botnets was described and included the simple and complex service offerings available from CaaS providers. Some of the key takeaways from the research are as follows:

"Originally robot networks were designed and used to enlist as many nodes as possible in criminal campaigns. Traditional botnets focused on intrusion and data theft to perform the following activities:

- Remote control of systems.
- Interruption/denial of service.
- Personal information theft (identity/personal credit/banking).

[131] As discussed in Chapter 1 and 2.

[132] https://www.fssecure.com/en/web/labs_global/botnets

[133] https://github.com/Visgean/Zeus

[134] https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet/

- Over time, botnets began to incorporate other services:
- "Doxing"/cataloging/selling stolen information.
- On-demand targeting and access provisioning to corporate systems.
- Third-party malware installation (RATs or ransomware) on systems.

Today, botnets provide managed services that include:

- Anonymous communications routing and publishing.
- Access management to subscribed networks/computers.
- Help desk services: including 24/7 technical support.
- Payment services (for electronic funds transfers or "crypto" currencies transactions).
- Markets for "dark web" products and services.

The actors behind these botnets, the "botmasters," use these operations to serve a bigger collective of campaigns by renting access to others, as well as for personal gain. Traditional botnets were "owner operated," but as their financial success and reputation grew, they became organized. The evolution of botnets from botmasters defining services to subscribers demanding products and services, has led to a customer-oriented industry. Subscribers vary, but their interests are generally reflected by the malware types in modern botnets that include[135]:

- Personal information stealers (that) are targeted at consumers, most often through spam or phishing, and seek credentials and other personally identifiable information that facilitates identity and personal financial credit, banking, and trading theft.
- Corporate information stealers (that) are targeted at corporate employees or officers, commonly through phishing but also supported by social engineering techniques to target individuals or business functions that can facilitate the theft of human resources information, or credentials (and computer access) for financial (ERP/ACH/EFT) fraud and theft.
- Market information stealers (that) are delivered via targeted phishing, or use sophisticated marketing techniques such as "waterholing" by infecting advertisements served to websites frequented by particular industry readers, or business networking services that create trusted links between people upon request or via introductions through social media. These are usually targeted at corporate officers of public companies, lawyers or auditors, or employees of financial services institutions and related media services. Information stealers facilitate the theft of protected or sensitive market information that can be used for insider trading.

The malware used are common in their design, differing only in whom they target, which instructions they employ to harvest different types of information, and which control sites they communicate with. Defining the **type of crime is no longer about the tool(s) being used, but the evidence of activity.** This evidence exists fundamentally in only three places: the control servers where stolen information is stored and made accessible to subscribers, victims' financial (or trading) accounts where fraud has been conducted, and victims' computer artifacts where the history of

[135] https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet-part-2/

misuse can be assessed."

Unfortunately, because many cybercrime (e.g. organizational intrusions) investigations have historically focused on proving that computers were targets of the crime, too much effort has been put towards attempting to determine who conducted the intrusion by looking only at the type of code used after system access was obtained. This concept in the cyber community is known as "attribution." Many cyber security research and cyber incident response firms put together investigative incident reports without providing evidentiary information which supports their conclusions about who conducted the attack, or what the objective was (aside from the intrusion). The unforeseen and unfortunate result of these marketing materials has been the tendency by many in law enforcement and private organizations to develop investigative theories and make early investigative decisions based on these analysts, who seldom have criminal investigation experience.

As previously mentioned, focusing exclusively on the technical aspects of an intrusion event leads to tunnel vision that may exclude a determination of the actual crime that was committed. Attribution by "objective" is a useful effort- i.e. who benefits according to what they are after (business interruption, fraud, theft, social distortion, secrets, Personally Identifiable Information—PII—or credentials for resale, etc.) because it will lead to properly assessing and defining, in scope, the nature of an investigation. Attribution by code "identity" is a very difficult exercise and can only be done by associating to and as supported by other evidence collected from HUMINT, SIGINT, in some cases Money Laundering Intelligence (MLINT), and Open Source Intelligence (OSINT). Technical artifacts collected and analyzed in an investigation can be important to understanding what the risk of an incident is, particularly if the information or function the cybercriminal was after is in a controlled business function such as securities trading or payment transfers. However, if the focus of the investigation is to identify individuals based on ELINT alone, then the validity and scope of the investigation will be too narrow and could potentially miss entirely the risk to other functions of government, commerce, or social stability.

The "SWIFT hacks" of 2016[136] reflect the issue of scope perfectly. Unauthorized accesses, attributed to botnet malware, facilitated the (mis)use of proprietary interbank payment network applications to commit wire fraud of tens of millions of dollars. Offshore accounts[137] were used to route and launder funds, after which cash withdrawals were accomplished by coordinated cybercriminals. The cybercrime(s) were much more than the botnet intrusions into the banks: they included humans with specific knowledge of banking processes and procedures, and apparently disparate organizations (of botmasters and subscribers). The scale is currently unknown as the activities have been replicated by different criminal organizations; however, the scope is apparent in the amounts in funds transferred and stolen through the wire fraud crimes.

Traditional crimes are assessed according to who has "Means, Motive, and Opportunity" - and who benefits. Investigators should assess the scope of cybercrimes as a starting point. To do so, it is first important to understand their nature. The nature of cybercrimes is represented in the figure below.

[136] http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C

[137] http://www.theregister.co.uk/2016/06/28/swift_victim_ukraine/

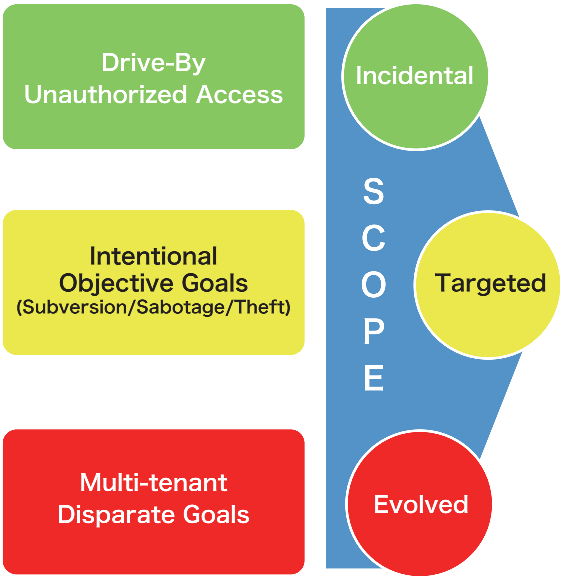


Figure 4-6. Nature of Cybercrime

Incidental

Incidental cybercrimes are committed as an "afterthought" or as the result of developing and deploying tools such as phishing or waterholing to "hook" victims. They are not intentionally targeted but may generally focus on themes or sites that certain demographics/industry sectors are more interested in than others. Incidental cybercrimes usually represent simple unauthorized access, such as CFAA violations, or "trespassing".

Targeted

As opposed to incidental cybercrimes, targeted cybercrimes are intentional and specific to objectives - or to people. In other words, a person may be the target for exploitation, or an organizational function (finance, legal, human resources, IT, or etc.) may be the target. Targeted cybercrimes can employ similar tools such as phishing, whaling (when targeted at executives), or waterholing – but they specifically target individuals, organizations, or groups that represent objective competitive or substantive interests.

Targeted cybercrimes have specific goals and objectives such as subversion (causing reputational or operational disruption), theft (stealing information, gaining market opportunities from protected information, or financial gain), or sabotage (destroying access, use, or continuity of operation). It is important to note that these objectives can be targeted at systems, facilities, and/or personnel – uniquely or coincidentally.

Evolved

Evolved cybercrimes are those that occur as a result of combined incidental and targeted activities. For example, as mentioned previously, a cybercriminal interested in committing fraud in a specific bank might choose to simply subscribe to a botnet service on the Darknet where computers belonging to that bank have been compromised by independent third party hackers and added to a BaaS service provider catalog.

Cybercrimes are not only committed from outside an organization through the use of botnets, custom tools, or crafted attacks. There is an often overlooked culprit that cybercrime investigators should be aware of, which is the role a potential insider may have played that allowed a third party to gain unauthorized access in order to commit a crime. Insiders can be individuals within an organization who are recruited by criminal or foreign intelligence organizations to assist with electronic access to bank account information, economic data, or military secrets. They can be found in the supply chain that all organizations rely on each day to function. The supply chain is defined as the people (e.g. contractors or subcontractors), processes (e.g. data storage services), suppliers, and technology (e.g. software) needed by an organization to conduct commerce or carry out their mission in service to the public.

Insiders and supply chains have significantly expanded the threat, impact, and scope of cybercrime in several ways:

1. **Insider threats:** Employees or individuals with insider access- particularly to key information technology systems, enterprise resource planning (ERP), databases, financial/treasury reporting, and research and development (R&D)- pose a significant risk and are frequently targeted for exploitation. Insiders may intentionally or unintentionally leak sensitive information, misuse their privileges, or utilize unapproved software services, and are susceptible to well-crafted phishing attacks. They may engage in malicious activities such as data theft, corporate espionage, sabotage, or fraud. Insider threats can be particularly challenging to detect, mitigate, and investigate as insiders often have legitimate access to systems and may bypass traditional security measures. Because of the easy access to the massive amount of breached data, cybercriminals have everything they need to build dossiers on individuals to target for access.

The 2023 ransomware attack on MGM Resorts located Las Vegas, Nevada, is a perfect demonstration of an insider threat-enabled attack. MGM Resorts' estimated losses are in the hundreds of millions of dollars. The attack, perpetrated by a ransomware group known as Scattered Spider (aka Roasted 0ktapus, UNC3944 or Storm-0875), was carried off as follows:

> "A social engineering attack allowed the threat actor to burrow into the MGM environment and establish a foothold. Due to the common mistake of password reuse…the attackers had usernames and passwords from previous data breaches. With additional information collected from a high-value user' s LinkedIn profile, they hoped to dupe the helpdesk into resetting the user' s multi-factor authentication (MFA). They were successful."[138]

Malicious insiders also can include disgruntled employees who contribute to data loss or business interruption events. Such was the case at Citibank in 2013:

> "At approximately 6:03 p.m. on December 23, 2013, an employee knowingly transmitted a code and command to 10 core Citibank Global Control Center routers, and by transmitting that code, erased the running configuration files in nine of the routers, resulting in a loss of

[138] https://www.cyberark.com/resources/blog/the-mgm-resorts-attack-initial-analysis

connectivity to approximately 90 percent of all Citibank networks across North America."[139]

2. **Supply Chain Attacks:** Supply chain attacks involve targeting third-party vendors, suppliers, or service providers to gain unauthorized access to an organization's systems or data. Attackers usually exploit vulnerabilities in the supply chain or gain access through compromised credentials to infiltrate trusted networks and cloud environments, compromising the integrity of software, hardware, or firmware. Supply chain attacks can have far-reaching consequences, impacting multiple organizations and industries. For example, a compromised software update distributed by a trusted vendor could lead to widespread data breaches or system disruptions.

   One of the more well-known and destructive supply chain attacks, which started in September of 2019 and was not discovered until December of 2020, occurred due to the compromise of software company SolarWinds. A summary of how the threat actors, believed to be tied to the Russian Government in an act of cyber espionage, carried off the attack is as follows:

   > "The threat actors hijacked the software compilation process for the platform and placed a backdoor inside legitimate, digitally signed Orion software updates. Those poisoned updates were pushed out to thousands of customers over several months. The threat actors exploited some of those backdoors to breach U.S. government agencies, such as the Departments of Justice and Homeland Security, as well as technology giants, including FireEye and Microsoft."[140]

   The size, scale, and scope of the attack is still not completely understood as the information and access gained by Russian actors, presumably working for the intelligence service, will and most likely has been utilized in subsequent intelligence gathering and espionage efforts. The attack had such a devastating impact to several U.S. Government organizations that the U.S. Securities and Exchange Commission (SEC) sued SolarWinds in October of 2023.[141]

   Investigators must consider how each aspect of the supply chain could be exploited by miscreants to carry out objective crimes. For example, many public and private organizations hire internationally-based IT product and services firms to build major applications supporting some of their most profitable business segments. These firms may go to great lengths to disguise their true ownership and affiliation to, or cooperation with, government intelligence services (or competitors, or criminal organizations). Such firms have seized on the increasing demand for software development by organizations that rarely employ a thorough vetting process before hiring vendors or related contractors. These procedural vulnerabilities have allowed nefarious firms to obtain contracts, develop systems, and ensure client organizations remain reliant on their technology – all while facilitating uninterruptible access to protected information, often

[139] http://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shut-down-90-of-firms-networks-across-america

[140] https://www.techtarget.com/searchsecurity/ehandbook/SolarWinds-supply-chain-attack-explained-Need-to-know-info

[141] https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html

including other partners, customers, and/or vendors related to the supported organization. If employees or affiliates of such firms commit cybercrimes, the scope of their access and activities can be massive.

3. **Increased Attack Surface:** Insiders and supply chains both increase the attack surface of organizations by providing additional entry points for cybercriminals. Insiders may have access to sensitive data and systems that external attackers cannot easily compromise while supply chain partners may have connections to multiple organizations, allowing attackers to pivot between networks and launch coordinated attacks. The rapid expansion of work from home due to the Covid-19 pandemic, the rapid adoption of cloud environments, and the authorized use of personal devices for professional duties has expanded the number of entry points for attackers to exploit. Gone are the days where organizations can easily map, manage, and limit the inventory of their network and infrastructure to simply company issued devices, servers, routers, switches,. and Internet/Intranet access in the buildings they own. The points of vulnerability that security teams cannot completely manage [i.e. home routers, Internet of Things (IoT) devices, gaming systems, etc.] are being exploited by cybercriminals given the ease with which these systems can be accessed due to bad security habits (e.g., use of default passwords on home routers). These devices are jumping off points for cybercriminals to access other systems.

Cybercrime Risk Targeting

Because of the increased anonymity presented by cybercrime, there has been significant effort put towards trying to define cybercriminals as being either “organized crime” or “nation-state” actors, and much of the determination on where to place the investigation is predicated solely on who was targeted (e.g. a financial institution) or the type of cyber tool which was utilized, such as a “banking Trojan”[142].

The tools, tactics, and procedures utilized by cybercriminals only facilitate the attainment of their objectives. Unfortunately, very little consideration is given to the concept that crimes of financial purpose, such as securities fraud or market manipulation, could serve differing agendas – including financial, competitive, reputational, and even political ones. To add to the confusion, there has been an evolution in strategies employed by miscreants to combine cyber tools and tactics as a means to distract incident analysts and investigators from the true purpose of the crime. This tradecraft has been observed in many DDoS attacks[143] as well as with ransomware attacks as mentioned in Chapter 2. While the tradecraft utilized by criminals is relatively new in the virtual world, the behavior is no different from distractions employed by criminals in real-world situations – such as robberies during demonstrations.

The blended use of historically separate cybercrime events has already moved into a model which will allow other types of nefarious activity such as the ability to subscribe to a DDoS or ransomware

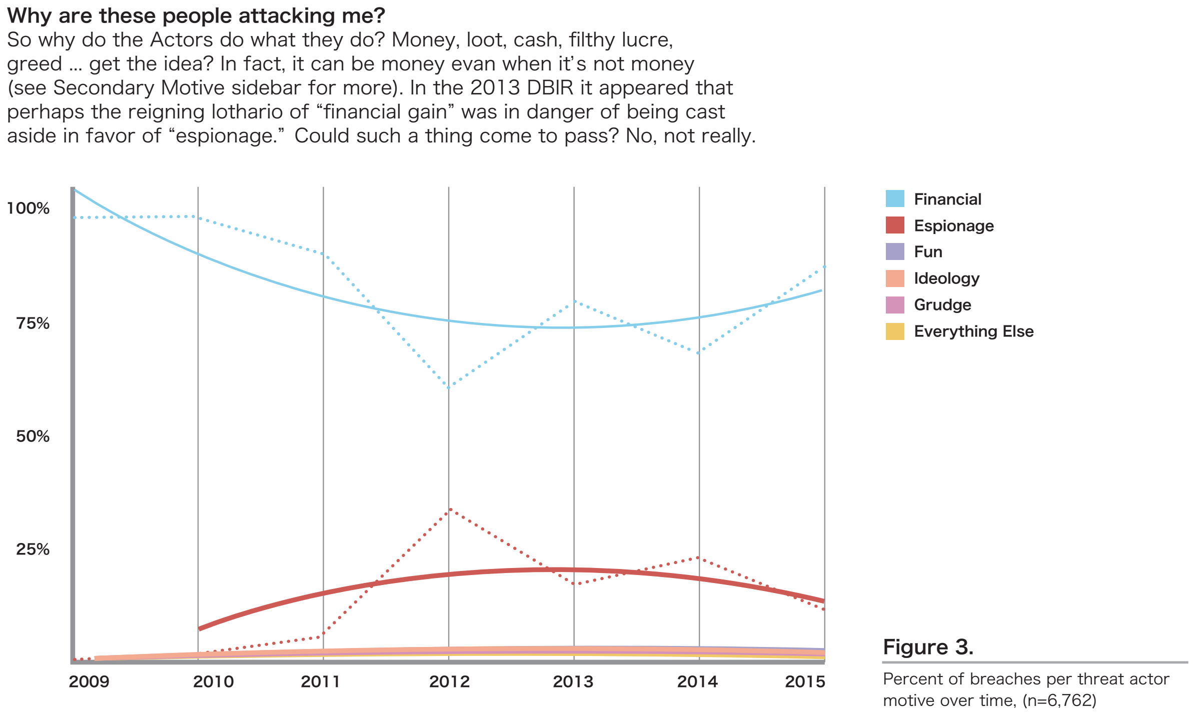
[142] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

[143] http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html

service for the purpose of driving business interruption or an advantage over a competing enterprise – such as described by cybercriminals who claimed to have been hired by an industry competitor to deploy "Jigsaw" ransomware into a company[144] in order to delay the release of a competing product. Another example of this type of activity was the enforcement action taken against a scouting director of a U.S. Major League Baseball team for gaining unauthorized access to a competing team' s player database and email system[145]. In one of the most significant examples of evolved cybercrimes, rogue traders hired hackers to steal non-public financial and operating performance information, enabling the traders to make futures trades in the "contracts for difference" market, ultimately netting more than $100 million in illegal profits[146]. The availability and ease of use of cyber tools has made it possible for even the least technically-proficient people to have an opportunity to commit crimes utilizing cyberspace.

Each year cyber security and research firms such as Trend Micro, Dell SecureWorks, Intel Security/McAfee, and Verizon predict, based on monitoring and research, the types of cybercrimes which will cause the most harm to public and private companies and, by extension, the economy. The headline statistic and associated chart in the 2016 report issued by Verizon[147] estimates approximately 89% of all breaches thus far have had financial or espionage objectives.

The following charts from the Verizon report indicate the trends of why and how cybercrimes are occurring.



Why are these people attacking me?
So why do the Actors do what they do? Money, loot, cash, filthy lucre, greed … get the idea? In fact, it can be money evan when it's not money (see Secondary Motive sidebar for more). In the 2013 DBIR it appeared that perhaps the reigning lothario of "financial gain" was in danger of being cast aside in favor of "espionage." Could such a thing come to pass? No, not really.

Figure 3.
Percent of breaches per threat actor motive over time, (n=6,762)

Figure 4-7. Cybercrime Motivation Trends

[144] https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf

[145] http://www.cbsnews.com/news/former-st-louis-cardinals-executive-pleads-guilty-to-hacking-houston-astros

[146] http://www.forexfraud.com/forex-articles/sec-terminates-cyber-fraud-ring-that-netted-$100-million-in-cfd-trading.html

[147] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

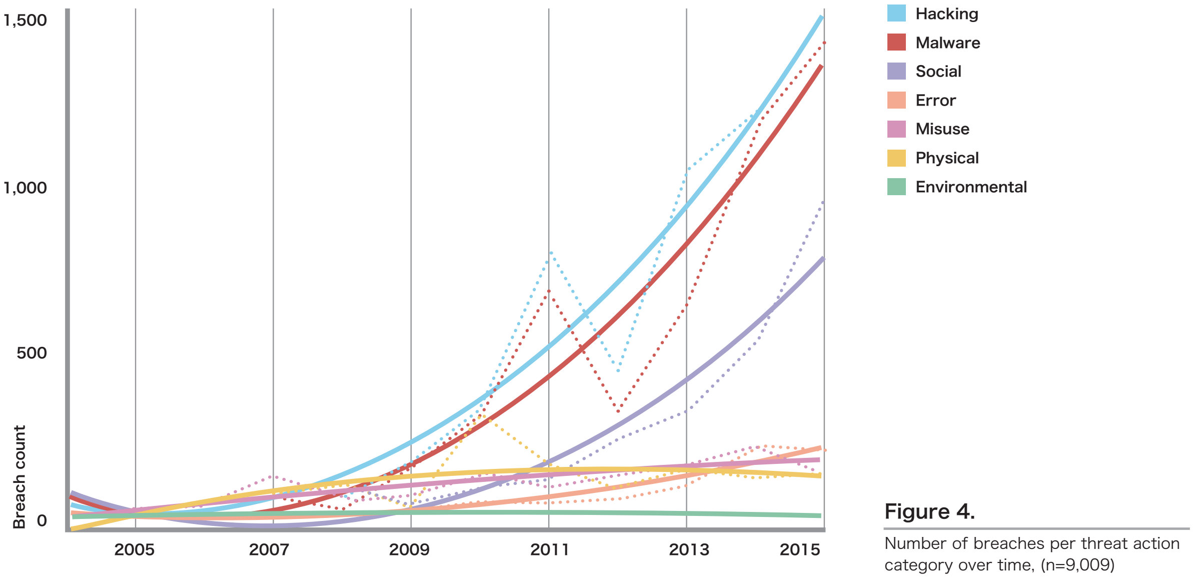


Figure 4-8. Trends in Techniques Employed in Cybercrimes

The use of computers and the Internet (tools) to achieve cybercrime objectives has dramatically increased since 2007 (according to the data with qualification in the report about sources and analysis). Since 2010 the objectives have generally been the same. Financial and espionage objectives have a converse trend association, although financial cybercrimes are trending upward since 2013 (and coincidentally espionage, at least as tracked in the report, has trended marginally downward). Technology has not created a new type of crime to investigate, it simply has altered the way in which crimes such as fraud, theft, money laundering, and espionage are being committed. Technology provides tools but hacking requires an objective that targets a risk or vulnerability. The vulnerability to be exploited may be procedural, technical or a person.

If an investigator can't answer the **what, how**, and **when**, then they won't successfully prove or disprove **who** committed the crime. However, determining the risk targeted to achieve the objective of a cybercrime is not an isolated event which only takes place at the beginning of an investigation. Most investigations change course based on the types of evidence collected, and many times the investigative approach is redefined. Accordingly, determining the "scope" of an investigation by the nature of the cybercrime and the risk(s) targeted for exploitation to achieve cybercrime objectives is paramount to efficiently and effectively bringing investigations to a resolution. These investigative principles are as relevant, and in fact, more important today as they relates to cybercrime, especially given the cloud of ambiguity most cases are initiated under.

The tendency during most cybercrime investigations is to define the nature of the investigation based only on the tools used in the commission of the crime, such as the case of malware (type, system attributes & functions) and the act of intruding or gaining unauthorized access to a computer and in some cases multiple computers in a network. Defining the nature of, or focusing an investigation based solely on, the tools used to gain access rarely will result in proving the most critical objective of an investigation, which is fundamentally determining **who** committed the crime. The equivalent in the physical world is to limit the scope of a murder investigation to only proving the type of weapon which was used. Or in the example of a white collar investigation, only proving the type of telephone used in the commission of a scheme to fraud.

Because of the tendency to place cybercrime into its own separate category, there has been an attempt to brand the activity. New terms like "Advanced Persistent Threat" (APT), "Distributed Denial of Service" (DDoS), "Malware", "Ransomware", "Doxing", "Drive-by Downloads", "Water-holing", "SPAM", "Phishing/Spear-Phishing", "Business Email Compromise" (BEC), "Adware", "Exploitation Kits", "Exfiltration", "Back-Connect", and others have created a separate vernacular, which for many law enforcement officers can be intimidating to comprehend.

Each new term associated to cybercrime can usually be related to established criminal activity, or items used in the commission of a crime. Some examples are as follows:

Tables 4-1. Association of Traditional to Cyber Crimes

Cybercrime Term	Equivalent Crime or Item used in Commission of a Crime
Advanced Persistent Threat	Espionage
Distributed Denial of Service (DDoS)	False Imprisonment (business)
Malware	Illegal firearms
Ransomware	Extortion
Banking Trojans—aka Botnets	Bank robbery
Doxing	Harassment
Drive-by downloads	Drive-by shooting
Watering-hole attack	Deception
Phishing & Spam	Telemarketing fraud
Spear-phishing/social engineering	Pretexting
Business Email Compromise	Fraud
Adware	False Advertising
Exploitation Kits	Home Invasion
Exfiltration	Theft
Back-Connect	Illegal Wire-tap

Cybercriminals have objectives. Contrary to social media attention, they don' t randomly execute attacks just for "lulz"[148]. Their motivations are sometimes simple, more often complex – as are the personalities that drive the actions that groups (of whatever organization, whether close-knit or loosely affiliated) have. Even rogue individualists who proclaim anarchy have objectives. These objectives represent risks or vulnerabilities that they seek to exploit. The association between the nature of cybercrimes and risks commonly targeted are depicted in the figure below.

[148] http://arstechnica.com/security/2015/01/come-for-the-lulz-stay-for-the-hacktivism-a-new-book-on-anonymous-reviewed/

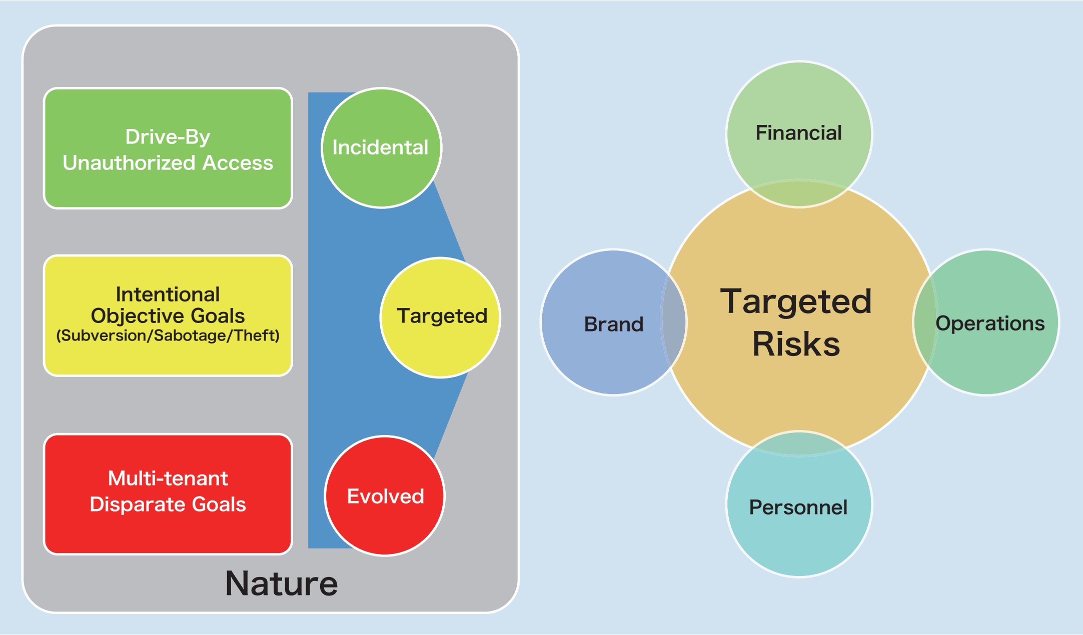


Figure 4-9. Association of Nature and Risks to Scope

There are many individual vulnerabilities that could be exploited in organizational (or personal) targets but the following categories of risk summarize the primary interests of cybercriminals – whether independent, organized, or sponsored (such as by nation-state or hired for purpose).

Financial

Financial risks represent not only direct commercial financial agreements and processes, but market financials as well. These may include vulnerabilities targeted to steal or commit fraud/misrepresentation of personal, corporate, budgeted (institutional), or market financial accounts and instruments. Financial theft and fraud can occur with banks and securities broker/dealers or related exchanges. They may involve "fiat" or virtual currencies – including credit instruments. The objective target of financial risks is to interrupt the ability to meet financial commitments or liquidity requirements that an organization or individual has. In some cases it may be simple theft from financial accounts, in others it may involve manipulation of corporate financial reporting or insider trading on non-public market information that can move sentiment (and corresponding confidence) in a public instrument such as stocks, bonds, or futures contracts on commodities (e.g. "short" or "long" positions used by hedge funds as insurance on trading positions[149]).

The scope of financial cybercrimes is subject to the nature of compromise activities. Incidental compromises may harvest accessible credentials from a system and deliver them to botmasters for their use or sale to interested third parties. Targeted and evolved compromises are substantial risks that since 2014 have been the primary focus of organized cybercrime (and ostensibly of nation-states functioning as such) groups. The scope of financial cybercrimes is individual or organizational, but may include partners and customers according to the inter-networking that exists. Entire markets (financial and commodities) may be at risk of financial cybercrimes, depending upon the profile and market access/prominence of the victim.

[149] http://www.investopedia.com/university/hedge-fund/strategies.asp

Brand

Cybercriminals often seek to devalue victim brands, or market confidence in a target, in order achieve their direct (competitive) or indirect (market) impact goals. The intent of targeting brand vulnerabilities is ultimately to expose non-public and potentially embarrassing or harmful information in order to reap some intended benefit from the activity. This may simply be “DOXing” executives and their salaries[150] or private communications, or may involve sensitive information release in forums such as WikiLeaks[151].

The scope of brand-oriented cybercrimes is predominantly oriented to corporate agreements, sales information, operational data, human resources information, and executive or client communications. Cybercrimes that target brand vulnerabilities are typically targeted, but since 2012 have increasingly emerged as evolved activities – as the infrastructure that is created by targeted attacks has certain residual value to other interested parties, and the access (and sometimes collected information or descriptions of catalogued sources) is made available through Darknet services. Brand-oriented cybercrimes can impact not only the victim but also associated personnel, customers, and partners.

Operations

Operational vulnerabilities are most commonly targeted by cybercriminals of varied motivations. Anyone can perform a DDOS attack against a target organization with a single computer by subscribing to a Darknet service or by building a commodity botnet to do so. Similarly, nearly anyone can use commodity tools and publicly-available information about target organizations’ systems to perpetrate targeted attacks and compromise activities. As many malware (simple to complex, as useful to the cybercriminal) are available publicly or can be purchased with customized capabilities in Darknet sites, operational vulnerabilities can be exploited by nearly anyone. The objectives of operations targeting are fundamentally to interrupt, disrupt, or destroy systems and organizational processes (or people in cases involving extortion). Besides DDOS, ransomware, “wipers”, the hacking of routers or email/web services, and “PBX overload” [152] attacks are commonly employed to exploit operations vulnerabilities.

Cybercriminals typically target operations vulnerabilities in order to achieve their own activist or competitive objectives – or to facilitate third-party objectives by distracting organization’ s investigators and responders from more significant cybercrimes. The scope of operations cybercrimes may accordingly be an entire organization, an industry segment, or might (if CaaS) represent a distraction from a financial or brand/competitive objective. It is important to assess not only what appears to be happening in an incident, but what else might have occurred. Operations-oriented cybercrimes are such common distractions in today’ s cybercrime activities[153] that investigators should always investigate “what else” is happening.

[150] http://time.com/3615160/sony-hack-salaries/

[151] https://wikileaks.org/

[152] http://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf

[153] http://www.computerweekly.com/news/4500253349/Most-DDoS-attacks-hiding-something-more-sinister-Neustar-warns

Personnel

Risks to personnel may be direct threats such as extortion demands, or indirect vulnerabilities that cybercriminals seek to exploit – such as stealing their personally identifiable information to commit identity fraud or financial/securities fraud with their accounts. Personnel risks that are exploited by cybercriminals are also sometimes "ephemeral" such as credentials theft achieved with botnet malware that enable their use of corporate systems and applications for fraudulent (or information theft) purposes.

The scope of personnel-oriented cybercrimes depends upon the nature of the activity. For example, incidental compromises of systems and credentials occur with nearly every current type of malware and with common phishing "lures" employed by social engineers. Targeted compromise activities rely upon more interactive and interpersonal social engineering (or procedural vulnerabilities in training and security awareness such as "fake help desk" calls or links in messages). Evolved activities are most concerning in terms of scope of compromise as they are based upon select intelligence that cybercriminals have employed to target specific individuals or functions of an organization in order to achieve their objectives. Although there will likely be fewer individuals targeted, the methods employed will be more esoteric (less visible to investigators) and the benefits to the cybercriminals both less attributable as well as more specifically significant (having more impact on the victim organization or individual).

Public vs. Private Organizations

Many of the risks discussed in the preceding section are common in both public (i.e. government) and private (business) organizations. A fundamental difference between the two types of organizations exists, though, in the perception and importance of risk categories.

The difference exists due to priorities and the ability of the respective organizations to address (or prevent) cybercrimes that occur. Shane Shook (executive editor of this book) describes the difference in an 2014 article as[154]:

"In the public sector that essentially means differentiating between which activities can be prevented, versus what activity should be captured and investigated. In the private sector the risk threshold is different, in effect relating "cyber-security risk management" to commercial considerations of what will affect the business – health and safety, financial, competition, brand, legal, and operational issues. Both public and private sector organizations are concerned with these issues but a fundamental difference is the ability of the organization to investigate – in terms of resources, methods, and legal jurisdiction to do so."

The following image (from the article) reflects the risk priorities of respective organizations. Although financial and operational risks are not reflected in public sector risk priorities, they are underlying management concerns – unlike the market concerns that private sector organizations

[154] https://info.cylance.com/incident-response-and-malware

continuously manage.

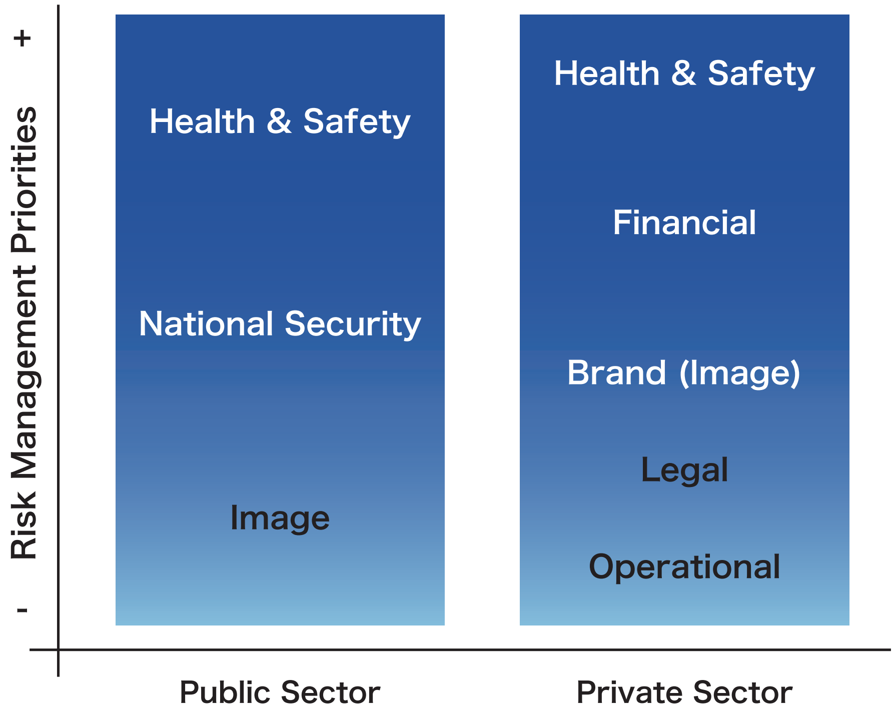


Figure 4-10. Comparison of Public and Private Organizations Risk Priorities

Chapter 4: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

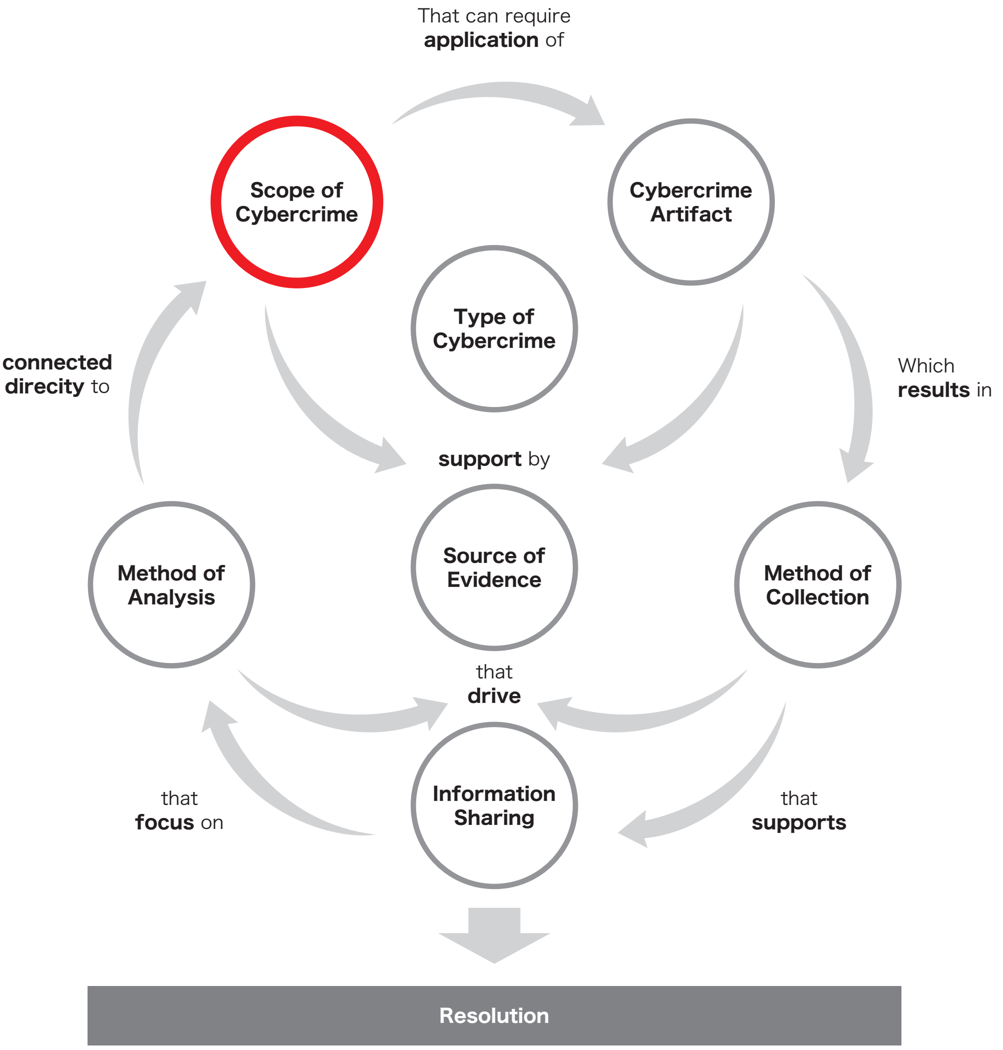


Figure 4-11. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 4-12. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 4-13. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

<legend>
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a strategic understanding of nature and risks targeted by cyber criminals and their intended objectives according to how they are organized.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. The type(s) of cybercrime and scope of affected systems, organizational functions, and personnel will be determined by evidence.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well as information sharing according to the type of cybercrime committed. Determining and understanding the scope of cybercrime activities is a strategic imperative to judiciary efforts.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The scope of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when, according to which organization/functions/personnel are affected.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 4: Review

1. What are the different “natures” of cybercrimes?

   Answer: Incidental, Targeted, Evolved

   Examples: Drive-by phishing/waterholing, targeted “whaling”, subscription to CaaS

2. What organizational functions do cybercrimes target?

   Answer: Financial, Brand, Operations, Personnel

   Examples: Financial Performance, Competitive Marketing, Logistics and Supply Chain, Human Resources

3. How have insiders and supply chains expanded the threat and impact of cybercrimes?

   Answer: easier/better access through trusted resources means uncontrollable impact

   Examples: Tesla, SolarWinds, JPMC market manipulation

4. How do risks to those functions differ in public versus private organizations?

   Answer: Financial and Operational risks are not specifically detailed in Public organizations

   Examples: Public organizations utilize budget allocations as cost centers whereas private organizations allocate budget as revenue/cost associations to profit and loss

Case Study 4: When Insiders Hack the Market

- **Crime:** Market Manipulation, Disinformation
- **Suspect(s):** Bank Trading Executives
- **Means:** Misuse of authorized access
- **Motive:** Personal gain
- **Opportunity:** Inadequate financial systems controls

In a landmark case that spanned eight years and involved thousands of unlawful trading sequences, two former precious metals traders at JPMorgan Chase & Co. (JPMorgan), Gregg Smith, and Michael Nowak, were recently convicted of fraud, attempted price manipulation, and spoofing[155].

From May 2008 to August 2016, the defendants engaged in a widespread spoofing, market manipulation, and fraud scheme. By placing orders they intended to cancel before execution, they were able to manipulate prices on the orders they wanted to execute on the opposite side of the market, effectively injecting false and misleading information about the genuine supply and demand for precious metals futures contracts into the markets.

Following a three-week trial, both defendants were convicted on several counts, including attempted price manipulation, spoofing, commodities fraud, and wire fraud affecting a financial institution. These convictions were a part of a wider effort by the Justice Department to hold Wall Street financial institutions accountable for undermining public trust in the integrity of commodities markets.

Smith and Nowak, alongside other traders at the JPMorgan precious metals desk, orchestrated a deceptive scheme that spanned from May 2008 to August 2016. This involved placing orders they intended to cancel before execution to manipulate prices on orders they planned to execute on the opposite side of the market. This practice, commonly referred to as "spoofing," was done to inject false information into the market about the genuine supply and demand for precious metals contracts.

The affected contracts were traded through the New York Mercantile Exchange Inc. (NYMEX) and Commodity Exchange Inc. (COMEX). The impact of this manipulation had far-reaching effects on the market, undermining the trust of investors in the integrity of our commodities markets.

Further to the conviction of Smith and Nowak, two other former traders, John Edmonds and Christian Trunz, were convicted in related cases, underscoring the extent of this fraudulent activity within the organization. Significantly, in September 2020, JPMorgan admitted to committing wire fraud in connection with unlawful trading in the markets for precious metals futures contracts and U.S. Treasury futures contracts. As a result, the company entered a three-year deferred prosecution agreement, agreeing to pay over $920 million encompassing a criminal monetary penalty, criminal disgorgement, and victim compensation.

This case underscores the importance of market integrity, demonstrating the serious consequences of such elaborate fraudulent schemes. It is a stark reminder to financial institutions of the legal and reputational risks involved in unethical market manipulation practices. The critical role of regulatory bodies and law enforcement agencies in upholding market integrity and protecting the trust of

[155] https://www.justice.gov/opa/pr/former-jp-morgan-traders-convicted-fraud-attempted-price-manipulation-and-spoofing-multi-year

investors is also evident from this case.

Chapter 5

Sources of Evidence

Introduction

Chapter 3 explored the artifacts of cybercrime according to the indicators associated with stages and TTP' s of cybercrime activities. As discussed, every crime leaves evidence behind. Some evidence is available in public sources because cybercrimes are often committed with shared services on the Internet, distributed actions (either for-hire or by organized criminal groups), or repeated in different forms – revealing TTP' s to investigators and analysts who share related information. Other evidence is solely available from internal (victim) sources such as systems, personnel, and associated activity logs.

The growth and adoption of cloud services (as third-party infrastructure) and subscription services since 2013 has led to changes in the scope of digital evidence. In addition to servers and end user computing devices such as desktop, laptop, and handheld and mobile computers, IAAS, PAAS, and SAAS configuration and use history logs are also important sources of evidence in modern cybercrime investigations.

Dramatic data and services breaches have been exposed and are related to cybercrimes including consumer payment card theft, bank account fraud, business email compromise, trading systems manipulation and fraud, and other crimes related to user accounts takeovers or exploits of services software vulnerabilities.

Additionally, as organizations have increasingly recognized cybercrimes as a threat to sabotage, subvert or steal,- they have correspondingly adopted monitoring and detection defensive tools to respond to attacks and breaches, and to investigate compromises. Subsequently, threat actors have increasingly modified their own approaches to "live off the land" and utilize "fileless" tools and scripts rather than installing recognizable backdoor trojans or other malware. The need for operating system and application services observability, network monitoring, and memory forensics has expanded the sources of evidence while investigating cybercrime incidents.

Not all cybercrimes are limited to the manipulation of end-user computers. The "internet of things" (IoT) includes industrial and building automation systems, as well as operating systems supporting varied industry functions such as call centers, fulfillment and shipping centers, traffic control, and logistics management. Since 2013, a correlated rise in attacks on these systems has occurred. Additional considerations for sources of evidence are now required to investigate cybercrimes involving those functions and their supporting systems.

This chapter will examine the external and internal sources of evidence available to investigators to understand the scope, impact, and actions of cybercrimes. This information will help organizational policymakers and managers develop audit and assessment criteria to define associated policies, systems, and procedures for defense and protection.

At the conclusion of this chapter, readers will have understanding of:

- What sources of evidence exist to identify cybercrime?
- Where can such evidence be found externally and internally to an organization?
- How do evidence sources differ in content, reliability, and structure?

Topic in Artifacts of Cybercrime

Figure 5-1 displays topic categories in the “Artifacts of Cybercrimes” knowledge domain.

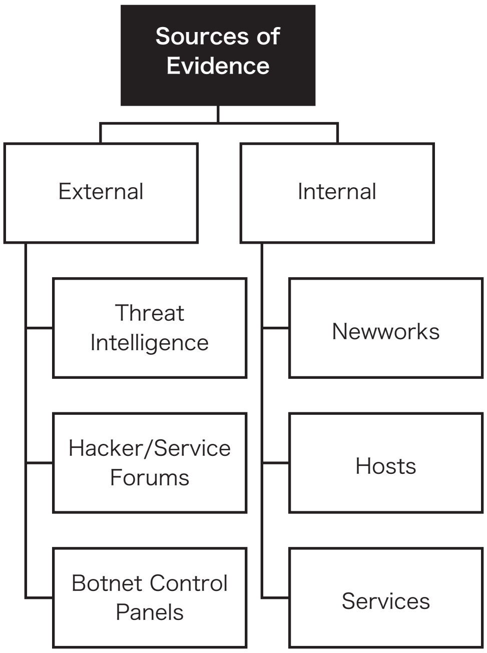


Figure 5-1. Topic Categories in the “Sources of Evidence” knowledge domain

What are Sources of Evidence?

Indicators and artifacts that help determine evidence have been discussed in prior chapters, according to the nature and type of cybercrimes. This chapter will describe where such information can be found and utilized to support investigations as evidence.

Sources of evidence include external and internal information and are derived from investigation, intelligence collection, and related analysis. Information is only as complete as the data that is collected, correlated, and understood through analysis. To provide useful information about cybercrime incidents, the sources of evidence should therefore be complete and timely. The following figure details some common sources of evidence available to an organization, to assist in the investigation (or detection and prevention) of cybercrimes.

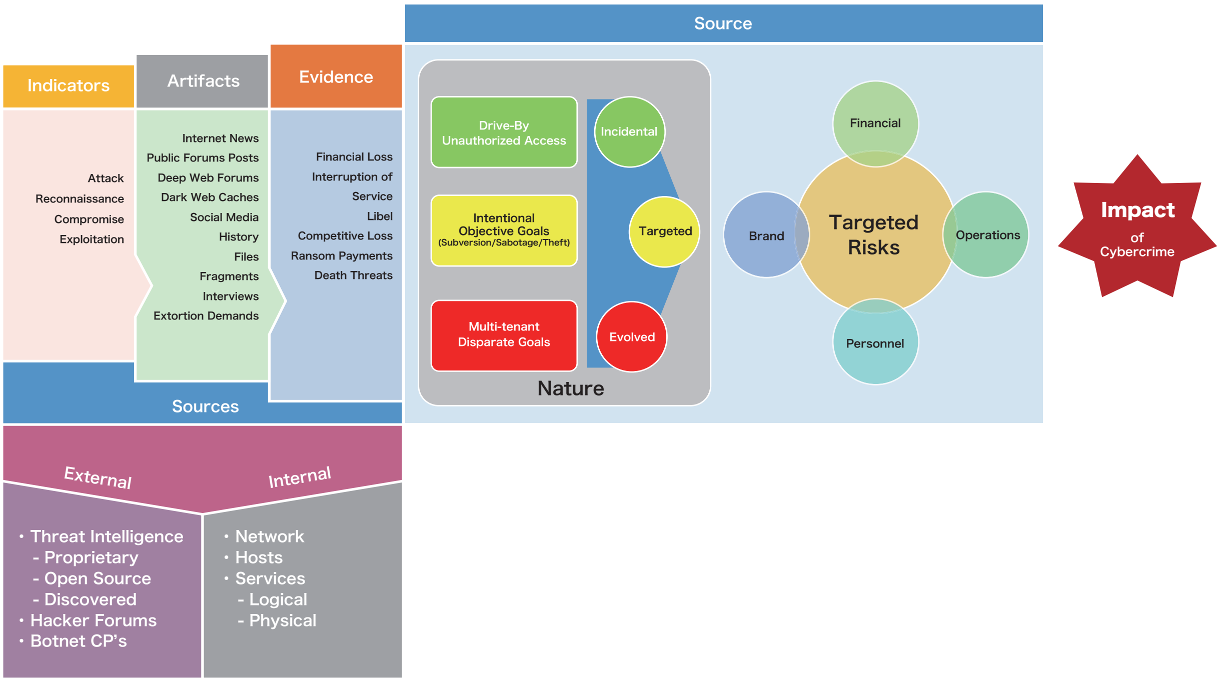


Figure 5-2. Association of Sources of Evidence

Every case of cybercrime is different; thus, the specific sources of evidence will change. Certain general categories of evidence are useful to examine, as computers and the networks they correspond with will retain artifacts and indicators of activities performed by cybercriminals. It is important that investigators consider all available evidence sources and properly evaluate the crime(s) committed according to the scope (as discussed in chapter 4). An investigator should think critically about how they might obtain information that is logged and how to hunt down intelligence utilizing the sources available to them.

External Sources of Evidence

External sources of evidence are paramount in a cybercrime investigation. When considering available sources, an external source is defined as evidence that originates from outside the victim' s organization. External sources of evidence provide a wide spectrum of relevant data-points to assist in identifying cybercrime activities. Accessing these sources mostly involves tracking down and monitoring publicly accessible (and sometimes more private) data sources online. Most of these activities exclusively involve digital intelligence gathering, while a small subset require some HUMINT (Human Intelligence) as well. .

External sources include many disparate sources of associable intelligence that support investigations. For example, the Japan Cyber Control Center (JC3) is an inter-agency cooperation described as "a non-profit organization seeking to reduce cyber space threats by creating cooperative frameworks between the industrial, academic and public sectors. JC3 promotes a pre-emptive, comprehensive response to cyber threats by capitalizing on the individual strengths of industry, academic research institutes and law enforcement agencies, and the police's stronger investigative rights. JC3's ultimate aim is to encourage cooperation and information sharing among relevant institutions worldwide, so they can pinpoint the source of any threat, and localize or minimize any resulting damage."[156]

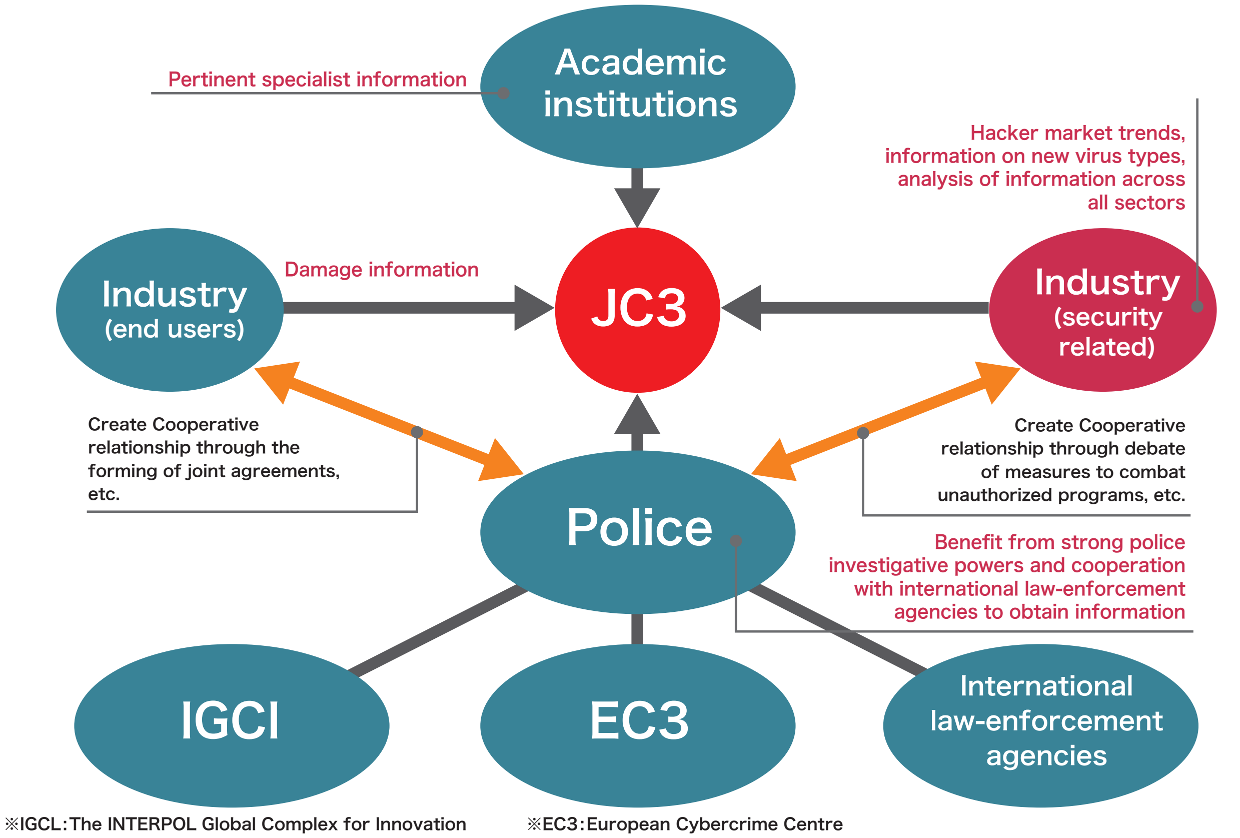

Pertinent specialist information
Academic institutions
Hacker market trends, information on new virus types, analysis of information across all sectors
Damage information
Industry (end users)
JC3
Industry (security related)
Create Cooperative relationship through the forming of joint agreements, etc.
Create Cooperative relationship through debate of measures to combat unauthorized programs, etc.
Police
Benefit from strong police investigative powers and cooperation with international law-enforcement agencies to obtain information
IGCI
EC3
International law-enforcement agencies
※IGCL:The INTERPOL Global Complex for Innovation
※EC3:European Cybercrime Centre

Figure 5-3. Japan Cyber Control Center Model

[156] http://www.nec.com/en/global/solutions/cybersecurity/efforts/index.html

There are three main categories for external evidence sources that are typically sought during cybercrime investigations: Threat Intelligence packaged by a 3rd party vendor or disseminated through Open Source or Proprietary Sources (including the organization' s own Threat Intelligence practice), forums used by hackers and CaaS providers, and - one that is often overlooked - botnet control panels used by botmasters and cybercriminals for command and control (C&C) communications and subscription services.

Threat Intelligence

An investigator will have many external sources of information available to them, but knowing how to obtain and process the information into high quality intelligence takes time and expertise. Until information has been collected, assessed for value (reliability and applicability), and interpreted to the scope of intended or observed criminal objectives, it represents "raw" intelligence. At best, it may represent risk intelligence. Only the interpretation and application of raw intelligence to investigative procedures to discover sources of evidence will reveal threats.

In practice, the overarching term "Threat Intelligence" refers generally to anything from simple IOCs, such as a collection of hashes of malicious software, URLs hosting malicious code, and IP addresses related to C&C servers (see above). Threat intelligence (TI) should also provide unique TTPs for threat communities/actors, behavioral patterns that can be applied to monitoring network and host behavior in an organization (related to exploitation, lateral movement, C&C and exfiltration), and other unique artifacts that are more tailored to the protected organization. Most common TI services/feeds can be utilized to ensure that evidence collection systematically covers the detection and identification of criminal evidence (hence the IOCs). More advanced TI services often require additional fine-tuning to profile the protected organization, and, more importantly, to identify and generally profile the threat communities relevant to the organization. Specialized sources of intelligence are available from HUMINT and ELINT as previously described in Chapter 4.

●Information vs. Intelligence

Threat Intelligence can be an important source of evidence to provide supporting details in an investigation. With the flood of information available at every analyst' s fingertips, the challenge is in differentiating between information and intelligence. Information can be described as data that has been aggregated from almost any source. It refers to raw, unfiltered data that may or may not be relevant. Information may or may not be true and must be critically evaluated. An investigator should never act solely on information.

Intelligence, on the other hand, is information that has been provided by reliable sources and a reputable track-record with proven accuracy and relevant data. Typically, intelligence is evaluated by several trained analysts before any kind of action (interruption, interdiction, or remediation) is planned.

The art of collecting intelligence of all forms has been around for centuries, but cyber threat intelligence capabilities and offerings are recent innovations. This growing field is producing increasing amounts (and sources) of proprietary intelligence (PROPINT), available to the public for a nominal fee. Other intelligence sources called open source intelligence (OSINT) provide similarly reliable information for free. Other sources with less specific reliability offer intelligence "tips" or untested information and are known as rumors intelligence (RUMINT).

●Intelligence Sharing Groups

Several law enforcement and government agencies offer threat intelligence to the public as a liaison service. Similar to the JC3 model mentioned previously, the U.S. FBI has a partnership with an organization called InfraGard[157], allowing members of the public with an interest in protecting themselves and their organizations against cyber threats to share intelligence. These groups have membership requirements but are traditionally free or are offered at a significantly lower price than offerings from threat intelligence vendors. One consideration when relying on government sponsored intelligence is that it is often more out of date than paid services.

●Types of Threat Intelligence

Several key types of intelligence may be provided by sources. While the quality and reliability of intelligence will vary depending on the source, intelligence can broadly be categorized into one of four areas:

- **Tactical Intelligence** - Tactical intelligence pertains to attacker tools, tactics, and procedures (TTPs). These indicators are useful for attributing specific tools and methodology to a particular type of threat.

- **Technical Intelligence** - Technical intelligence typically involves indicators of compromise related to malware and communications protocols. For example, malicious files or communications may have unique characteristics or may be associated to monitored activities which can be attributed to cybercriminal organizations.

- **Operational Intelligence** - Operational intelligence focuses on the immediate operating environment, as well as threat actor capabilities and intent. Specific details about an upcoming attack or an active compromise are considered operational intelligence.

- **Strategic Intelligence** - Strategic intelligence includes higher-level details that provide value to senior management when measuring risk and planning organizational threat response structures and budgets.

●Proprietary Intelligence (PROPINT)

Proprietary intelligence provides evidence from services such as the intelligence sharing groups noted above or other vendors. Marketed cybercrime threat intelligence is a growing field with varying quality.

- **Vendors** - Several private industry companies and affiliated groups such as FS-ISAC (financial), H-ISAC (healthcare), and RH-ISAC (retail) offer their customers controlled access to proprietary intelligence. These sources of intelligence vary widely in completeness and comparability, and may or may not contain open source intelligence that is also available for free.

[157] https://www.infragard.org/

- **Security/Law Enforcement** - Non-profit (government or public) security and law enforcement groups offer proprietary intelligence to subscribers who meet criteria for acceptable access and use. These sources include a mix of raw and outdated intelligence (due to classification and handling restrictions).

●Open Source Intelligence (OSINT)

Open source intelligence is collected from publicly available sources. While this intelligence is not always tested for reliability, it is a free source of data created through "crowdsourcing". OSINT can be gathered from any number of available external sources, but is often derived from the following areas:

- **Search Engines** - One of the most used and widely available sources of information is search engines. Information is indexed by search engines which constantly scan and index accessible Internet pages, retaining information even if the site owner removes the data. By simply utilizing a search engine, it is possible to parse through large amounts of data for very specific pieces of intelligence. Many investigators utilize advanced search engine features, often called "**dorking**"[158], to reduce the volume of search results through custom query syntax.

  ◦ **People Search** - People search services specialize in identifying individuals by aggregating as many sources of public information as possible. People search services often scrape public records including property ownership and legal records. These search services can be incredibly effective in identifying additional details about a suspect or group of individuals.

  ◦ **Image Search** - Image (and reverse image) search services are a feature of many search engines. They allow an investigator to find co-occurrence (according to confidence factors) of images in shared social media profiles or web pages. Often, the evidence of a cybercrime may include "consequential artifacts" of the use of technology such as fragments of a video chat or background in a picture. Image search services can be utilized to discover such important details.

- **Social Media** - Social media use has grown significantly over since 2013. By utilizing social media, information about individuals and organizations can be gathered to build profiles for an investigation. Additionally, social media service users often do not fully understand how to restrict access to their information allowing the information to appear in search engine results. These details can assist an investigator in identifying a suspect, their interests, and others who they might be in communication with. In some cases, cybercriminals will tout their "1337 h4x0r skillz" (elite hacker skills) or taunt victims and law enforcement (sometimes through ignorance or from a misperception of their anonymity in the social network) using social media services.

●Discovered/Rumors Intelligence (RUMINT)

RUMINT comes from many sources including observations, confidential informants, interviews,

[158] https://www.exploit-db.com/google-hacking-database/

malware and communications reverse engineering analysis, and the reconnaissance or monitoring of forums and similar sources. It is “RUMINT” until it can be determined that the source(s) is reliable and can provide structured and useful intelligence repeatedly. Thereafter, it will either continue to be RUMINT or may be integrated into PROPINT or OSINT source collections.

Forums and Message Boards

Hackers and criminals socialize and engage in information exchanges on the Internet. The vehicles used to facilitate such communications are often online forums with varying degrees of access control. This includes the lower hanging fruit of “open” forums where one simply needs to create a login to access the relevant portions, all the way up to highly restricted and vetted forums where in order to participate an existing forum member with good standing needs to vouch for the new forum member, and often new members must exhibit some proof of their hacking (or other criminal) capabilities and criminal endeavors.

Forums and message boards are a preferred method of communication for cybercriminals. They may offer a number of illicit and/or illegal services and goods. It is not uncommon for attackers to discuss upcoming targets on forums in order to collaborate and enumerate useful details. By monitoring these forums, intelligence can be collected to support investigations and prevent developing attacks or compromises. Forums are unusually productive sources of critical intelligence, but forum members are wary of law enforcement and security researchers “lurking” in their domains. As a result, HUMINT from confidential informants or members of forums is sometimes more dependable.

Botnet Control Panels

Most cybercrime operations utilize tools that employ some kind of centralized facility for controlling hijacked or compromised assets (computers or mobile devices). Even if a cybercriminal has direct (virtual) access to assets via the internet or a network connection, the scale of their activities usually depends upon access to many distributed computers or devices – whether for purposes of obscurity or necessity.

Access control and “botnet” maintenance is supported by C&C servers with control panels that automate certain tasks. Those tasks include delivering malware tools on demand to engage computers in the botnet with custom configurations for remote control and operational support of cybercrime activities. The control panels also have script repositories to commit configuration changes to bot “drones” (computers under control of the botnet). They additionally store information stolen from drones, such as configuration (and hence victim) details and data or audio/video recordings. Some control panels simply route stolen information to other storage hosts and may incorporate varied intermediary proxies and routes to obfuscate the control panel host’s server location.

Botnet control panels can be a critical source of evidence as they include artifacts containing specific details about malware use (both scripts for task execution and compiled tools for remote access and control), victim identifying information (IP address, system configuration/build, computer name, etc.), victim data (screenshots, video/audio recordings, files, etc.), and metadata related to the operation (and duration) of the botnet. The control panel may also contain correspondence configuration details that can help investigators discover the scope of cybercrime activities (and objectives) across geographies and their organization. Law enforcement has historically attempted to merely interrupt or “takedown” botnets by capturing C&C servers. However, it has become evident that control panels are a critical, detailed source of evidence and intelligence that investigators should utilize when feasible (or allowed).

Internal Sources of Evidence

When reviewing potential sources of evidence, it is critical to consider all available sources of information and data residing in an organization' s networked systems during the investigation. Similar to a traditional crime scene, internal evidence is defined as anything investigators can use as evidence without needing to leave the scene of the crime. In digital forensics, the crime scene is considered the systems and network devices that correspond with a suspect system. Digital forensics, however, is only one activity in cybercrime investigation. Investigators should also consider physical (facilities and equipment) and human sources of evidence in an organization.

As the information security community evolves, an increasing number of organizations are adopting a "defense in depth" model, or a "layered approach to security". This involves identifying areas of high risk within an organization and putting proper security controls and mechanisms in place to either prevent or detect an incident, though it certainly does not imply immunity from cybercrime. By building up defenses at several critical locations within an organization' s IT network, it is possible to reduce the overall impact a single attack vector or security mechanism failure might create.

In addition to IT, organizations employ "Operations Technology" (OT) to support facilities and production activities. OT may be simple control systems such as power, water, environmental controls, and security/safety systems, or may include complex production management equipment using programmable logic controllers (PLC) or remote terminal units (RTU) to operate and maintain related equipment. Information security and corresponding cyber investigations policies and procedures should be aware of and incorporate both IT and OT.

The following figure provides a simple display of internal sources of evidence investigators should evaluate.

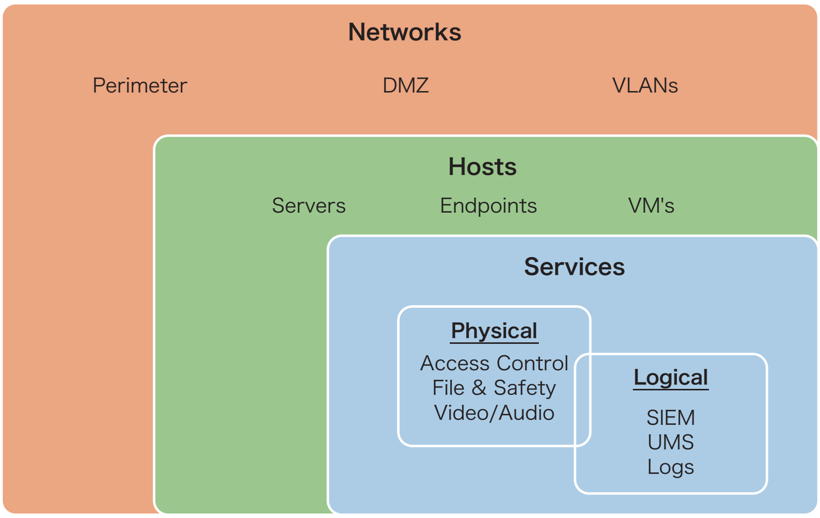


Figure 5-4. Internal Sources of Evidence

Networks

Organizations employ several types of network configurations. These include perimeter, services, network zones, virtual and physical “local area networks” (VLANs), and a “demilitarized zone” (DMZ) that separates each from the other either by physical or logical segregation using firewalls, routers and bridges as needed to facilitate organizational communications. Networks convey not only data but also voice, video and audio communications. The architecture of how such communications are served may be coincidental or separate (i.e. a PBX/phone system network may be integrated into the LAN or perimeter network services, or may be entirely separate). Network equipment is essentially a computer with an operating system, services configuration, and maintenance tools or facilities. Whether it is a router, firewall, PBX, or video access-monitoring system, however, each piece of network equipment is a potential source of evidence that investigators should incorporate in their analysis. At the very least, each type of network system contains historical activity logs. These systems may also support or be supported by network recording (or packet-capture) tools that can assist investigators in understanding communications artifacts such as protocols, methods, timing and addresses of C&C related to cybercrime activities.

When evaluating which logs might prove useful in an investigation, it is important to consider how network based tools, applications, and security appliances can be leveraged to provide evidence to an examiner. Most of these devices can be configured to log events and actions that occur on a daily basis. If such logs are stored properly, they can be critical in identifying lateral movements within a network, the scope of compromised systems (and applications/credentials), and the nature of the cybercrime, according to captured network artifacts. The following network equipment can provide useful evidence or artifacts to support an investigation:

- **Perimeter Firewalls** – Perimeter firewalls provide evidence of outside-in and inside-out communications between the organization and remote services. The types of communication protocols used, the configuration of services allowed (or violated) by policies, and the frequency/timing of communications are useful details that can provide intelligence for IOC definition to tip-off activities. Such information is useful intelligence to share with related communities or services (such as ISACs or law enforcement).

- **Network Proxies** – Network proxies provide user and service activity histories. Web proxies are typically implemented to protect an organization's users from malicious websites and content not deemed necessary to business. These appliances typically log key details of communications artifacts such as the source computer address, time of connection, content type, remote service and address, and the direction of communications. Those details can be utilized by an investigator to identify who might have accessed a specific website, or in assessing a suspect’ s activities.

- **DMZ** - A network demilitarized zone (DMZ) is a physical or logical network that separates the Local Area Network (LAN) from other/remote networks. Systems in the DMZ are typically Internet-facing and are a common point of investigation in incidents involving compromised web servers and applications. Activities commonly observed in DMZ logs include vulnerability scanning, exploit attempts, and penetration from the DMZ into the internal network hosts. DMZ logs are often configured only to detect intrusions. However, “extrusion” detection is actually a higher value intelligence detail for collecting evidence of cybercrimes, as it can lead investigators to related systems where an assessment of intent or objectives can be performed.

- **Zone/VLAN Switches/Routers/Bridges** – Networks that serve different functions of an organization are often segmented into “Zones” or virtual LAN’ s (VLANs) for security purposes. To communicate between network segments, equipment to bridge the different segments are necessary. These network devices have configuration (and change) histories and may also log transfer connections between segments with date/time and source/destination addresses. They can provide useful artifacts for determining evidence of related cybercrimes.

- **VPN** – Virtual Private Network (VPN) routing equipment enables remote workers to connect with internal network hosts. Connection history details are logged both on the router as well as the host.

- **PBX/VM/IVR** – A Private Branch Exchange (PBX), often equipped with a VoiceMail (VM) and Interactive Voice Response (IVR) service, contains useful logs related to communications made through phone systems and remote accesses to recorded/available information. These systems can be an important source of evidence in “fake help desk” or extortion cybercrime incidents.

- **Safety/Security Systems** – Safety and security systems include fire, lighting, physical access control, and emergency notification services. These systems typically contain time-based event logs with correlated details such as control codes and badge/access codes that can help an investigator understand physical event activities associated with cybercrimes.

- **DCS (RTU/DCU)** – Distributed control systems (DCU) include remote terminal units (RTU) and data concentrator units (DCU) that control the operation of industrial control systems (ICS). These include programmable logic controllers (PLC) for production and logistics control systems as well as building management systems (BMS) such as power, water, heat, air conditioning, elevators, and automatic doors. Often overlooked in investigations, these systems contain logs that typically include access account histories (by date/time and credential) as well as connecting host addresses, and sometimes related protocol details. The artifacts available in such logs are useful for correlation with other cybercrime artifacts where “insider threat” activities are a concern in an investigation.

Devices capable of recording network packet captures (“PCAP”) files should also be examined. These devices can act as a Digital Recorder for network activity, allowing the investigator to reconstruct network activity. Forensic analysis of PCAP files has improved significantly over the years. It is now possible to recover data streams such as Voice/Video-over-IP (“VOIP”) and other communications from a packet capture. Other vital information such as usernames and passwords might also be obtained in a PCAP file, sometimes even if communications are encrypted.

Hosts

Endpoint systems (computers, servers, mobile devices, and etc.) contain a wealth of information for cybercrime investigations. Endpoints are typically a higher risk to organizations due to exposure they bring. Most endpoints have ubiquitous access to commonly-exploited services such as email and web browsing. By identifying focus areas of evidentiary significance, an investigator can create a procedure to systematically analyze these areas for information pertaining to the investigation.

A variety of tools to administer and maintain endpoint system health are pre-installed on all endpoints in a corporate environment. Software such as anti-virus often keeps log files identifying a history of malware or suspicious activities that a system has encountered. A compromised host with a history of malware might cause an investigator to reassess an incident timeline. Files such as host based firewalls can also provide great detail around suspicious network activity, brute force attempts, and the presence of malicious backdoors. Other beneficial sources of evidence might be contained in the software deployment history, which can hold key details concerning system patch and configuration history.

●Web History

Web browsing activity is commonly a valuable source of evidence. It can help investigators identify user activities to determine if any suspicious activity including malware infection, illicit content, and other information might provide context around an incident. Additional artifacts contained in the browser cache might also allow the reconstruction of websites including webmail. Items such as bookmarks and favorites can help an investigator understand some of the user' s regular web-based activities. In certain cases, it is possible to recover stored passwords from web history or browser settings. The recovery of these passwords might unlock additional evidence that was previously unavailable.

●Chat and Messaging History

The use of chat and messaging programs is very common, and understanding how and where the most popular applications store this information can be very helpful during an investigation. Several forensic analysis tools that attempt to reconstruct chat history, attachments, and related artifacts.

●E-mail and Calendar Artifacts

Reviewing email and calendar artifacts is incredibly useful in determining relationships between people or groups of people. Email records can often be recovered from the local system via offline mailboxes as well as from the server that hosts the mailbox of the user in question. The delivery of malicious email is a commonly-utilized method to infect endpoint systems; the analysis of malicious email metadata and content, including the links and file attachments within emails, can lead to the discovery of several types of attacks and intrusions.

●Address Books and Contacts Entries

Identifying who a suspect has contacted or commonly communicates with can be very informative. In certain situations, this information can link a user to an alias or contact methods they used such as email, social media, phone, or forums.

●Hidden and system files

Files with the "hidden" or "system" attribute are commonly found on Windows systems. However, if these are found in anomalous locations they should be examined as potentially suspect artifacts in an investigations. While applying the hidden attribute to a file is not a difficult task, an investigator must consider why a suspect might want to conceal the file from others users of the system. These files will not normally appear in directory listings or file system viewers unless specifically requested, and are usually overlooked by regular users.

●Compressed archives

Compressed archives (.zip, .rar, .7z, etc.) files and related histories are useful for identifying potential data exfiltration and tools left by a cybercriminal. Hackers often store the tools they use in a compressed file in order to avoid detection. In addition, multi-part compressed files are frequently used to exfiltrate data, as larger data sets require a series of smaller compressed files to avoid being detected by network security tools.

●Encrypted files

Encrypted files should be examined to determine their relevance in an investigation. Cybercriminals commonly employ encryption tools to avoid detection. While it may not always be possible to decrypt these files, it is worth examining each for useful information. Compressed archives are frequently encrypted.

●Deleted Files and Recycle Bin

Deleted files should be examined in "Trash" or "Recycle Bins" (depending upon the operating system) if accessible. If deleted files are no longer accessible, recovery of those files may be possible with forensic tools. In some cases, the history of the file(s) deletion can be recovered from other files and artifacts and should be examined. In particular, when a file was deleted, by whom, and what the contents of the file were (if possible to determine) are useful information to assist in determining evidence of a cybercrime.

●Temporary Files and Directories

Many applications utilize temporary folders as a location to write data being used by the program. Fragments of such files and related information can be found by reviewing data in these temporary folders. For example, word processing software creates temporary files in the event of an application failure. Temporary files can contain useful content to describe artifacts of a cybercrime or its objectives.

●Virtual Machines

The presence of a virtual machine on a suspect host should be treated like finding another system for forensic analysis. With the increase in popularity of virtualization, it is common to find virtual machines on both endpoint systems and servers. These systems will have the same forensic artifacts available as a physical machine and the entire disk structure will be present for analysis. In certain situations, such as when a virtual machine is found in a suspended state, the memory of the virtual machine is stored in a file on the local disk. Virtual machines can reveal useful details and artifacts of a cybercrime.

●Application and System Backup Files

Many investigators can attest to the quality of system and application backups. A proper system backup allows an examiner to review additional “snapshots in time” of a suspect system. With backups, it is possible to find previously deleted information. For example, if a user backs up their cellular phone on a related computer, it might be possible to access other artifacts that lead to evidence that wouldn’ t otherwise be available such as text messages, phone records, and other activities stored within the backup.

●Images and digital media

Depending on the type of investigation, examiners should review images and digital media content present on a system. In certain cases like system misuse, it might be useful to identify any illicit content or other media that has not been deemed necessary for business. Files sourced from and applications used to interface with Peer to Peer (P2P) networks should be analyzed for malware and potential piracy issues.

●Secure Deletion

Secure deletion tools are used to ensure a file is not recoverable by forensic investigators. These tools function by first deleting the target files and then overwriting the data on the disk several times to make recovery impossible. There are legitimate purposes for some of these tools, especially for sensitive data that is not to be shared. However, if these tools are discovered they should be reviewed against organizational policies to determine the legitimacy of their use.

●Remote Access Files

Remote access configuration and history cache files for system tools or applications such as “Microsoft Terminal Services Client” (MSTSC), “Virtual Network Client” (VNC), Secure Shell (SSH), Public TTY (PuTTY), Citrix, “LogMeIn”, “WebEx”, and “GoToMyComputer” can provide useful history and, in some cases, images or artifacts related to their use. These artifacts can provide valuable demonstration details to develop and assess evidence of cybercrimes.

●System Configuration Settings

Operating system and user services configurations provide a wealth of forensic details as sources of evidence in compromised hosts. Most forensic analysis and research information concerns Microsoft Windows configurations for the simple reason that most compromises related to cybercrimes (other than DDoS or distribution of malware, etc.) are committed against vulnerabilities in the Windows operating system or related applications, or take advantage of user behaviors through social engineering.

The registry hives for any Windows Operating System are a primary source of information about system activity and should be a focus of analysis when determining evidence of cybercrimes. The registry for a computer with the Windows Operating System is essentially a hierarchical database that stores configuration information for the operating system, applications, users, and hardware devices.

Registry “keys” that contain information about settings or use history contain a useful artifact for the “Last Write Time”. This information is not available via traditional viewing techniques, but with the assistance of forensic procedures it can reveal helpful information to support an investigation.

The following Microsoft Windows Operating System Registry Keys contain useful sources of evidence.

- **HKEY_CURRENT_USER (HKCU) –** Contains configuration information for the logged-on user. Artifacts that might be present in this registry hive include folder and display options, control panel settings, and the history of other user-specific activities.

- **HKEY_LOCAL_MACHINE (HKLM)** - Contains hardware-specific information that is required by the operating system. Key artifacts from this registry hive include information about mounted drives as well as system and application configuration keys. The HKLM sub-tree contains vital information about resources configured to support persistent services (including malicious Trojans).

- **SYSTEM** - Is primarily used for storing information about the Windows Operating system setup, network information such as DHCP lease details, and information on mounted file systems. The SYSTEM key also holds the “Plug-and-Play” device enumeration (history) as well as hardware drivers that are loaded into the operating system. Incidental “run” keys are also configured for persistence in the SYSTEM registry hive.

- **SOFTWARE** - Maintains variable configuration details for individual applications that are installed for all users.

- **SAM** - Contains detailed information about user account management and security settings for the local system. Encrypted (hashed) user passwords are also stored within the SAM key.

- **SECURITY** - Stores information about the security database of a domain the current user belongs to.

- **NTUSER.DAT** - Contains user application and profile configuration settings and use history. The use history includes mounted network shares, removable storage media and devices, application and file access history, and persistent or scheduled services details.

- **Most Recently Used Lists (MRU)** - Present throughout the registry and can be used to gain additional insight into a user’s actions. There are several different MRU keys that can be utilized by an investigator to assess the use of the computer. MRU keys contain information such as which documents or files were used and the timestamps associated with activities.

●Metadata

Metadata is “information about data”. It refers to attributes of files and their relationship to users or operating system and storage/device configurations. For example, documents contain metadata describing properties such as creation date, owner, and editor. Operating systems files such as the Master File Table (MFT) or related Operating System Journal Files contain “index” metadata that helps the operating system refer to the “file system” for user interaction. This is a critical source of evidence.

●Windows Prefetch/Superfetch Files

Microsoft Windows Prefetch files are designed to improve Windows and application start-up performance by loading application data into memory before it is demanded. . Initially introduced in Windows XP, Prefetch has since been integrated into subsequent versions of the Windows operating system. Details such as how many times a program has been run as well as the timestamp of the last execution are contained in Prefetch files.

Prefetch files contain dimensional clues about coincidental files and activities at the time of an application process execution. As such, they can provide investigators with important context to consider other artifacts of compromise, as opposed to the simple indicators of compromise that are focused on too often.

To demonstrate the depth of information available when evidence sources are considered in the context of the entire investigation, the following section outlines the potential usefulness of the Prefetch artifact, corrects common misconceptions around it, and clarifies how it can be utilized during investigations.

A Digital Forensic Analysis of the Windows Prefetch Artifact

Functionality

The prefetching process typically operates within the first ˜10 seconds of an application launch and monitors the files and directories with which an application interacts, with the goal of optimizing subsequent launches. The prefetch filename is structured as **<executable filename>-<prefetch hash>.pf** where "executable filename" is the filename of the original application truncated to 29 characters and "prefetch hash" is calculated based on the original filepath. Prefetch files are stored in the **C:\Windows\Prefetch** directory and each prefetch file (*.pf) captures data on the execution of a specific application including its file path, command-line parameters, previous times run, directories accessed, and interactions with other files.

When an application is re-executed, the existing Prefetch file associated with the file is referenced to facilitate performance improvement. The same file is also updated to reflect information about the current execution.

In Windows 7 and earlier versions, the operating system can store a maximum of 128 Prefetch files and in Windows 8 and subsequent versions, this capacity is increased to a total of 1,024 Prefetch files.

Correcting Common Misconceptions

There are several common misconceptions about the Prefetch artifact. The following is a list of clarifications to correct those misconceptions:

- Prefetch is NOT enabled by default in Windows Server operating systems.

- Prefetch does NOT capture every file accessed by an application during its execution. Instead, it focuses on the files and directories accessed within the initial (approximately 10) seconds of the application launch, aiming to optimize subsequent launches by preloading frequently accessed resources.

- While Prefetch records information about the execution of applications, it does not necessarily indicate that the associated files were executed. Prefetch records the files accessed during the application launch process, which may include dynamic link libraries (DLLs) and other resources loaded by the application but not necessarily executed directly.

- The 8-character hash present in Prefetch filenames is computed based on the application's file path and command-line parameters. This potentially results in multiple Prefetch files for a single application due to variations in command-line arguments.

- Prefetch may not accurately reflect application execution in certain instances - for example, in instances of manual deletion or corruption of Prefetch files and cases where applications bypass the Prefetching process.

Utilization in Digital Forensic analysis

Investigators can leverage Prefetch as generally reliable evidence of the execution of an application. The creation time (B[159]) of a prefetch file can be indicative of the first time that the binary was executed on the system, assuming previous Prefetch files were not removed or copied from its original location. The last modification time (M[160]) of a prefetch file can be indicative of the last time that binary was executed on the system. In all cases, a delta of 0-10 seconds will need to be subtracted from the creation and modification times to account for the Prefetching process times. Generally, smaller applications will load faster than larger applications.

Parsing Prefetch files can provide valuable insights into the files and directories accessed by an application during its execution. This is particularly prevalent in the context of examining malware and identifying attempts at exploitation, specifically in scenarios where malware attempts to load itself as a library component within an application.

Windows Prefetch serves as a valuable artifact for investigators, offering insights into the execution patterns of applications on Windows systems. By understanding its functionality, common misconceptions, and best practices for utilization, investigators can effectively leverage the Prefetch artifact and correlate it with other system sources like process execution data in Windows Event Logs or Shimcache to reconstruct a more precise timeline of application events.

●Paging file and Hibernation files

Microsoft Windows uses a memory caching file called “pagefile.sys” to store sections of memory

[159] Birth - indicates the file creation time in an NTFS filesystem
[160] Modified - indicates the file modified time

that do not fit into physical memory. An investigator can review the paging file to find artifacts and even recover files in certain cases. Windows also uses a similar caching mechanism called "hiberfil.sys" that is utilized when the computer goes into hibernation mode. This process stores active memory (RAM) to "hiberfil.sys" on-disk. Upon reboot/resume, the hibernation file resurrects the contents in memory. These files can be forensically analyzed to identify volatile memory artifacts such as system state, applications use, temporary files contents, and services/communications configuration and use details, all of which are useful for determining evidence.

●Volatile Memory Artifacts

Numerous methods for extracting and analyzing artifacts from active memory (RAM) have been created by forensic analysts. Random Access Memory is a form of "volatile" computer data storage. This means that the information in RAM is temporary, providing only a brief "snapshot" of information about the configuration of a system or user activities at a point in time.

It is important to consider the various types of information that might be contained in volatile memory artifacts. Active details about an application, user, or system function are available - for example, encryption keys, passwords, and other authentication tokens are present. Other volatile memory artifacts include:

- **Running Processes** - All running system processes, their configuration, and the use of associated resources. This information is similar to viewing the "Task Manager". Each of the processes will have an assigned Process ID and (credentialed) process owner.

- **Past and Present Network Connections** - Active and past network connections (and network services settings), including the port and destination of traffic, can be utilized to identify suspicious connections or activity on ports that should not be used.

- **User Names and Passwords** - User name and password information are stored in memory (either in clear-text if in current use or hashed for temporal use) for applications and services.

- **Encryption Keys** - Encrypted files and mount points constantly reference related decryption keys and are retained in active memory.

- **Open Registry Keys** - Registry hives are required for the operating system to function and are actively loaded into memory while the system is running. By analyzing hives from memory, it is possible to associate specific processes and system activities to a user or secure identity (SID) token. Many types of malware also utilize the registry to maintain persistence on a compromised host, so it is worthwhile to investigate suspicious keys that might indicate malware attempting to utilize run keys (or other keys) to survive a system reboot.

- **Screenshots/Console History** - Memory analysis techniques make it possible to reconstruct a screenshot and console history of commands entered in dialog boxes or command lines at the time of memory capture. With this evidence, it may be possible to determine other applications that are running or information present on the screen for active users.

- **Decrypted / Unpacked Applications** - Perhaps one of the most valuable aspects of memory analysis when reverse engineering malware is the ability to capture decrypted or unpacked applications and file segments. Any program file that is originally encrypted will need to be unencrypted to run properly. These artifacts can reveal important details such as the utility or resource dependencies of malware, as well as the C&C addresses and protocols for corresponding with Botnet Control Panels.

- **Memory Resident (Fileless) Malware** – Memory-resident (fileless) malware is becoming more frequent and does not leave any filest on the hard disk to indicate malware use, making traditional detection and mitigation much more difficult. Memory-resident malware will bypass many endpoint protection/detection software such as AntiVirus. By analyzing the memory of an infected system, it may be possible to identify malicious files loaded into memory supporting processes or directly injected into active processes.

●Cloud Based Storage

The use of cloud-based virtual computing and storage systems is becoming more widespread among cyber criminals, and this trend is likely to continue. Cloud computing does not offer the conveniences that the physical acquisition of evidence (disks) does. Cloud-based memory acquisitions are challenging because memory allocated to virtual servers and applications is shared with other virtual services.

There are still useful methods that can be utilized to capture cloud-based process and logical memory. However, virtual servers are often located in different jurisdictions than those which the investigator is operating from. When cloud storage based systems fall within scope of an investigation, investigators should ask questions regarding the accessibility of data, available logs, contracts or service-level agreements, and jurisdictional restrictions[161] that might aid or hinder the evidence gathering process.

A deep dive on cloud computing

Given the widespread adoption of cloud computing, a deeper examination of its foundational elements is warranted. While cloud technologies offer unprecedented flexibility and scalability, they also present unique challenges for investigators.

Cloud providers like Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure provide similar services with slight variations in naming conventions. These services include:

Cloud Console

The cloud console serves as the primary interface for managing and configuring the resources of a specific cloud services provider. It offers a centralized dashboard for administrators to oversee their infrastructure. The cloud console logs user activities, API calls, and configuration changes, providing

[161] See Chapter 1 for related information.

valuable insights into system events and user interactions. It is worth noting that each cloud provider has its own default logging and retention settings, with some providers charging for these services. As a result, customers may disable logging to reduce costs, a factor that must be taken into account during investigations.

Access to the cloud console and API is controlled by Identity and Access Management (IAM) policies. Essentially, IAM determines the permissions granted to users or service accounts, dictating what actions they can perform on specific resources within the cloud environment. This becomes vital evidence during investigations of unauthorized access to a cloud project, providing insight into activities carried out by attackers.

Cloud Storage

Each cloud provider has its own implementation of cloud storage services. For instance, GCP offers Google Cloud Storage (GCS), AWS offers S3 buckets, and Microsoft Azure offers Azure Blob Storage. Cloud storage buckets are governed by their respective IAM policies which regulate access to data. Additionally, these buckets can be configured to be publicly accessible for purposes like hosting public websites or documents. A common risk associated with these storage services is the accidental exposure of data due to misconfigured IAM policies, such as granting access to all public users.

Cloud providers offer alternative storage options such as Network File Share (NFS) and managed services like MySQL or Redis. In the event of an incident, it's crucial to understand if a cloud project contains any data, where it's being stored, and the nature of the data stored.

Virtual Machines

Virtual machines (VMs) allow for the creation of isolated computing environments within a physical machine, hosted in the data center of cloud providers. Snapshots of a VM's underlying disk can be captured to preserve original evidence which can then be analyzed using traditional forensic tools. Common file system formats in cloud environments include NTFS, XFS, and ext4.

Containers

Containers, popularized by platforms like Docker, are processes with added isolation and resource management. Containers use namespaces to provide isolation and cgroups to limit and monitor resource usage. Namespaces are a Linux kernel feature that limits what resources a process can see on the system. Cgroups is another Linux kernel feature that limits, accounts for, and isolates the resource usage of a collection of processes (e.g. CPU, disk, network).

Containers can run as either privileged or unprivileged. A privileged container's container user identifier (UID) 0 is mapped to the host's UID 0. A UID 0 is essentially root level access to the system. An unprivileged container, on the other hand, maps the container UID 0 to an unprivileged user outside of the container and only has extra permissions on resources that it owns itself.

Docker uses a client-server architecture in which the client allows users to send commands to the Docker daemon (dockerd) which then validates and sends the request to the runtime engine containerd. Containerd then helps set up the necessary isolation and sends the request to runc which helps create and run the container. A comparable approach can be expected for Windows based operating systems. The primary distinctions lie in how the Windows kernel manages virtualization, given that namespaces and cgroups are a Linux implementation. For further insights into this mechanism, refer to the referenced Windows Container Forensics blog[162].

From an investigation standpoint, since containers are running as processes, they will have a process id (PID) associated with them. The installation directories also contain some useful artifacts. For Windows, the default installation for Docker is typically **C:\Program Files\Docker** and for Containerd is typically **C:\Program Files\containerd**. For Linux, the default installation for Docker is typically **/var/lib/docker** and for Containerd is typically **/var/lib/containerd**. While the files contained within these directories can be examined manually (e.g. cat, grep), investigating containerized environments is easier when you are able to obtain the differences between the last known good state of the container and the changes (e.g. using docker diff). There are also open source tools capable of analyzing container images, including Docker Explorer and Container Explorer.

Kubernetes

Kubernetes, also known as K8s, is an open-source system for automating the deployment, scaling, and management of containerized applications. While both Docker and K8s are container technologies, they function differently. K8s is typically favored for production deployments, as it simplifies the management of containers across multiple servers. Containers in K8s are run in logical groupings called **pods**. You can run and scale one or many containers together as a pod across clusters (groupings of machines) commonly referred to as **nodes** within K8s. The K8s control-plane, analogous to a Docker Daemon, decides when and where to run pods, manages traffic routing, and scales pods based on resource utilization or predefined metrics.

Investigating a K8s cluster involves reviewing K8s control-plane logs and pods distributed across multiple nodes. A significant challenge with K8s is the dynamic state of pods and nodes running within clusters, and subsequently mitigating an attacker operating within the environment. For example, imagine credentials were exposed allowing an attacker gain access to the K8s control plane and schedule a malicious deployment. Analysis will consist of identifying what nodes the malicious pods were deployed to and determining whether they have been deleted due to K8s autoscaling. If the node is available, investigators can proceed to capture a snapshot of the underlying disk and subsequently examine the pods (the containers operating within the node). Mitigating such an attack would consist of resetting user credentials, deleting the malicious deployment from the K8s control-plane, and identifying all impacted nodes and what data they had access to.

Artifacts typically found on nodes include the underlying container engines such as **CRI-O, containerd, and dockerd.** Pod level logs are stored by default in /var/log/pods for Linux installations and in C:\var\log\pods for Windows environments.

Managed Services

Managed services and software as a service (SaaS) applications have become vital tools for organizations seeking to streamline their operations and enhance collaboration. Unlike traditional on-premises software deployments, SaaS applications are hosted and managed by third-party providers, eliminating the need for maintaining internal infrastructure. For investigators, SaaS applications are crucial sources of evidence in many investigations into employment law violations, business email

[162] https://osdfir.blogspot.com/2021/07/windows-container-forensics.html

compromise (BEC), phishing, fraud, and more crimes.

Notably, Microsoft 365 (O365) and Google Workspace stand as the most prominent SaaS offerings. Microsoft 365 (O365) offers a suite of productivity tools hosted in the cloud including Microsoft Outlook, Office, Sharepoint, and OneDrive. Logs are available from the Microsoft 365 Security and Compliance Center. Additionally, Microsoft Purview (previously known as Azure Purview) facilitates data governance and eDiscovery for users' O365 data.

Google Workspace, provided by Google, offers similar cloud-based productivity tools including Gmail, Google Drive, and Google Docs. Logs are available within the Google Workspace admin console. Additionally, Google Vault serves as an information governance and eDiscovery tool for Google Workspace. With Vault, you can retain, hold, search, and export users' Google Workspace data.

Investigating both O365 and Google Workspace environments involves analyzing user activity logs, email headers and exchanges, and file sharing permissions.

Utilizing Open Source Tools for DFIR

As the adoption of cloud services grows, so too do cloud-based digital threats. Organizations need to be able to respond quickly and effectively to security incidents. One critical component of incident response is having the right set of tools at hand to analyze and respond to threats.

In the realm of Digital Forensics and Incident Response (DFIR), there are numerous tools that cater to various aspects of the investigative process. While commercial solutions offer robust feature sets and dedicated support, commercial tooling can be cumbersome to deploy in Cloud environments due licensing that requires dongles in some cases. Open source tools have gained traction due to their accessibility and flexibility, and the collaborative efforts of a vibrant community of digital forensic specialists.

Open Source DFIR tools encompass a broad spectrum of functionalities, each serving a distinct yet connected purpose in a forensic investigation. While the array of open source DFIR tools is extensive, several main categories have emerged (with some tools fitting in multiple categories):

- **Collection**: There are several methodologies for the acquisition of disk images or individual artifacts. Conventional methods such as **dd** and **FTK Imager** can be employed to capture complete disk images, while specialized tools like **Google Rapid Response (GRR)** or **Unix-like Artifacts Collector (UAC)** can be utilized to obtain a subset of artifacts. However, executing a binary for collection on the host system is not a forensically sound approach. The selection of an appropriate method should be determined based on legal obligations and applicable regulations.

- **Live Analysis**: This process involves analyzing and monitoring memory, as well as performing live host analysis. Commonly employed tools for these tasks include **YARA** and **GRR**. These tools enable investigators to extract transient data such as active processes, open network connections, and system configuration settings. This provides real-time insight which is highly valuable for identifying memory-residing malware including script-based threats.

- **Processing**: Specialized tools such as **Plaso (log2timeline)** and **Bulk Extractor** are utilized for parsing and correlating digital artifacts obtained from hosts, encompassing system logs (syslog and Windows Event Logs), Windows Registry hives, application-specific logs, and other sources.

The available parsers for Plaso can be found in the referenced documentation[163].

- **Timeline Analysis**: Various tools aid in the timeline analysis of digital artifacts, sometimes serving both as processors and analyzers of artifacts. Notable examples include **Autopsy** and **Timesketch**, which are both widely utilized for artifact and timeline analysis. In certain circumstances, utilizing the command line tools 'cat' or 'grep' can provide the quickest results.

- **Indicator of Compromise (IOC) Tracking**: Open source platforms such as **Malware Information Sharing Platform (MISP)** and Yeti facilitate the tracking of IOCs identified during forensic investigations. By centralizing IOCs in a collaborative environment, these tools allow forensic specialists to track IOCs across their investigations.

With so many DFIR tools serving different yet connected purposes when solving an investigation, there is a need for a solution that streamlines the deployment and integration of multiple open-source DFIR tools. This helps reduce the time and effort required to set up, maintain, and scale an effective incident response infrastructure.

One new promising repository that aims to solve this is **OSDFIR Infrastructure**[164]. This is an open-source repository that provides a set of Helm charts and simplified instructions for automating the deployment and integration of multiple open-source DFIR tools in Kubernetes.

The repository supports the deployment of several popular open-source DFIR tools, including:

Figure 5-5. Open-source DFIR tools

- **Timesketch** - for collaborative forensic timeline analysis featuring analyzers to help identify patterns in data; support for Plaso, JSONL, or CSV file imports; and built-in integrations to tools

[163] https://plaso.readthedocs.io/en/latest/sources/user/Parsers-and-plugins.html
[164] https://github.com/google/osdfir-infrastructure

such as:

  - **DFIQ** for digital forensics investigative questions and approaches to answering them
  - **Sigma** for detection and hunting rules to run across timelines
  - **Unfurl** for URL graph analysis
  - **Yeti** for searching all available intelligence across timelines

- **Turbinia** - for automating forensic evidence processing at scale, helping find prevalent problems and including built-in integrations to many tools such as:
  - **Plaso (and related projects such as dfVFS, libyal, and SleuthKit)** for extracting data from a variety of sources into a correlated super timeline
  - **Container Explorer** for container level processing
  - **Docker Explorer** for docker container level processing
  - **Fraken** for multi-threaded YARA scanning
  - **Libcloudforensics** for mounting evidence from cloud platforms
  - **dfDewey** for string extraction, indexing, and searching tools that collect strings from files and raw disks and index them to be searchable.
  - As well as many more such as Bulk Extractor and analysis jobs of prevalent artifacts.

- **Yeti** - for DFIR and threat intelligence tracking, enabling responders to store and analyze CTI (observables, TTPs, campaigns, etc.) from internal and external systems.

- **GRR** - an incident response framework focused on remote live forensics.

- **dfTimewolf** - a framework for orchestrating forensic collection, processing, and data export, helping data passed along between tools. Examples include:
  - Creating a copy of a cloud disk, submitting the disk to Turbinia for further processing, and then submitting any timelines Plaso created into Timesketch.
  - Grabbing a filesystem timeline from GRR, using Turbinia to process the timeline by running Plaso, and then importing the created timeline into GRR.

OSDFIR Infrastructure helps to fill in gaps by streamlining the deployment, integration, maintenance, and scaling of multiple open-source DFIR tools. It provides the following key benefits:

- **Faster Deployment Times**: Deployment can take a few minutes, allowing responders to focus on more critical tasks.

- **Provides Consistent Configuration**: Integration occurs automatically, reducing risk of misconfiguration or human error.

- **Certified Deployments**: It eliminates to need to review documentation for multiple tools, reducing complexity from shared resources in a centralized way to learn about many DFIR tools.

- **Easy to Scale**: It can be installed on minimal resources, and any component can be modularly scaled with a single command. Kubernetes autoscaling is a powerful feature.

- **Improves Reliability**: It contains built-in Chart linting and testing, with more ways to run integration tests to catch issues between tools. Port-forwarding locally running applications is easy and reliable as well.

The benefits of OSDFIR Infrastructure are summarized in the diagram below which compares current processes that require a lot of steps versus a single simplified deployment through OSDFIR Infrastructure.

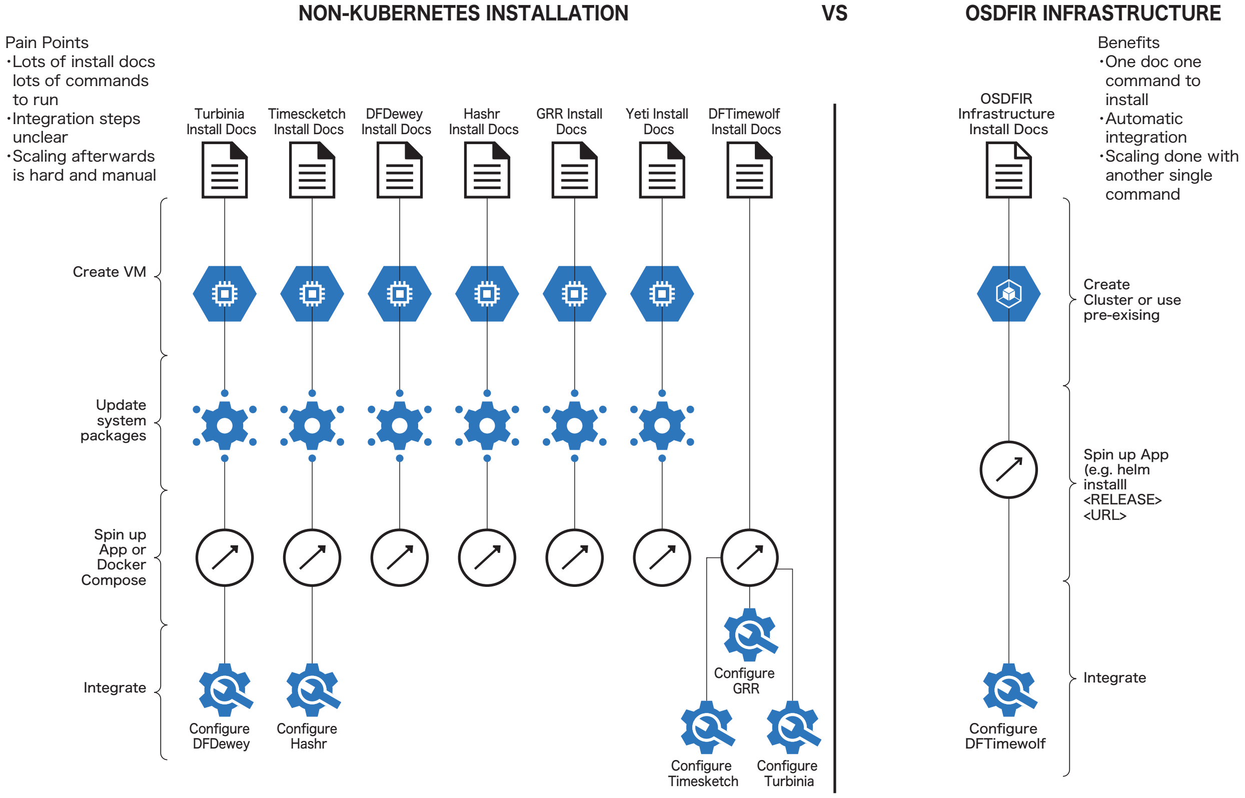

NON-KUBERNETES INSTALLATION
VS
OSDFIR INFRASTRUCTURE
Pain Points
·Lots of install docs lots of commands to run
·Integration steps unclear
·Scaling afterwards is hard and manual
Turbinia Install Docs
Timescketch Install Docs
DFDewey Install Docs
Hashr Install Docs
GRR Install Docs
Yeti Install Docs
DFTimewolf Install Docs
Create VM
Update system packages
Spin up App or Docker Compose
Integrate
Configure DFDewey
Configure Hashr
Configure GRR
Configure Timesketch
Configure Turbinia
OSDFIR Infrastructure Install Docs
Benefits
·One doc one command to install
·Automatic integration
·Scaling done with another single command
Create Cluster or use pre-exising
Spin up App (e.g. helm installl <RELEASE> <URL>
Integrate
Configure DFTimewolf

Figure 5-6. Comparison of non-Kubernetes installation and OSDFIR infrastructure

The following diagram depicts the configuration of a fully deployed OSDFIR Infrastructure stack:

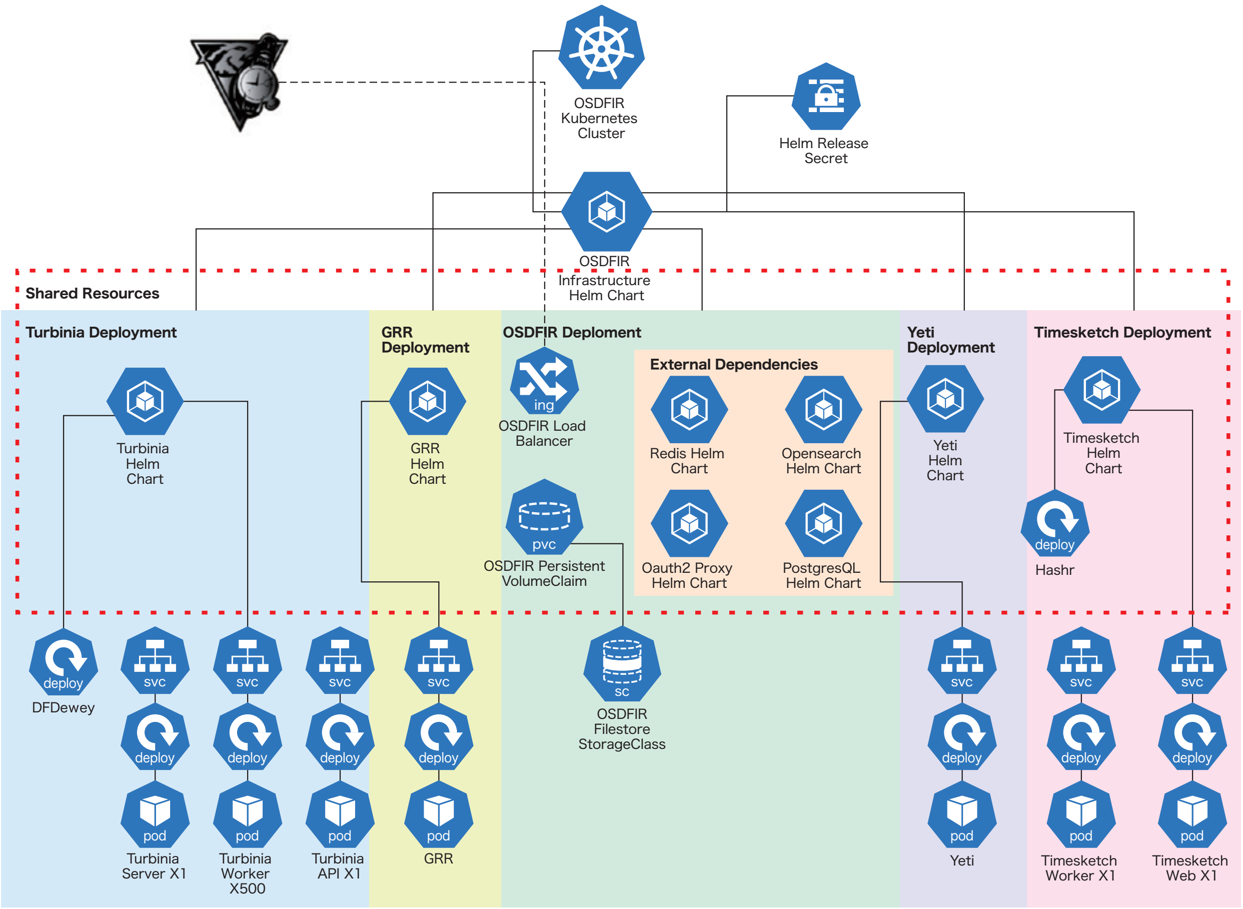


Figure 5-7. Fully deployed OSDFIR infrastructure stack

While OSDFIR infrastructure may appear complex at first, once the Helm client and K8s clusters are set up, deploying the entire infrastructure becomes a single-command process (including any necessary upgrades). The project is dedicated to streamlining this process by offering detailed documentation and implementing secure default installations. All applications run locally by default, allowing users to access them by following post-installation instructions provided in the Helm chart after installation.

Services

Logging systems and infrastructure may not be the most attractive aspect of investigation but are often critical in reconstructing the actions that occurred during an incident or building a timeline of events. There are many facets of log management that must be taken into consideration when evaluating the relevance of a log source. The availability and integrity of logs is fundamental to an investigation. In this section, many of the key characteristics of log management will be reviewed to provide insight into how each log might be utilized, along with common issues an investigator might encounter in the field.

●Event Logs

Microsoft Windows Event Logs can be delineated into two main groups: “Windows Logs” and “Application and Services Logs”. Within the “Windows Logs” classification, there are several types of logs organized by category.

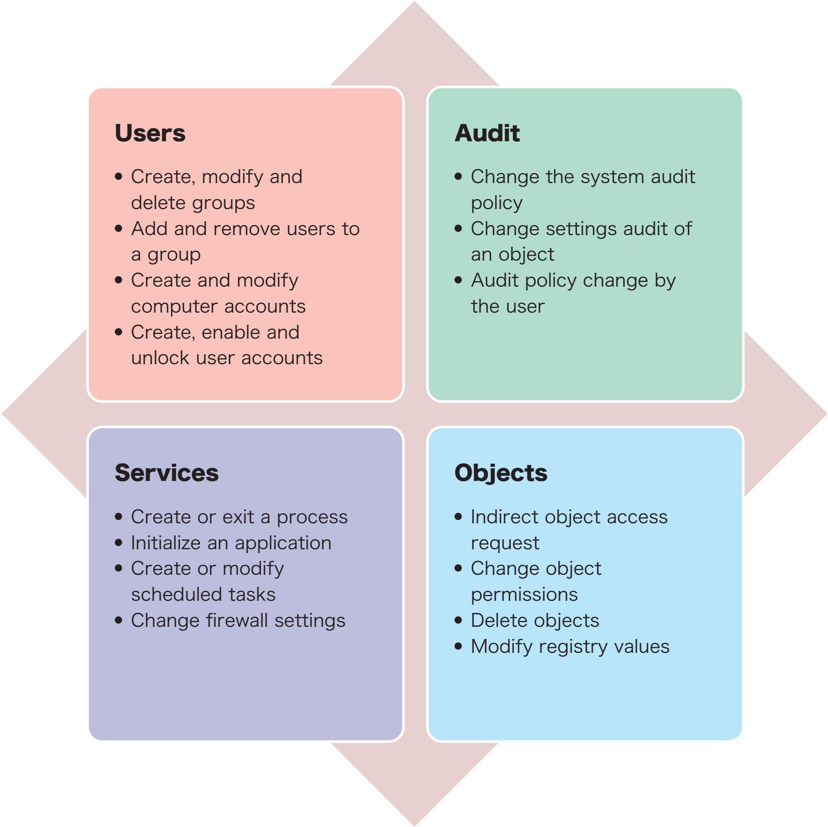

Users
• Create, modify and delete groups
• Add and remove users to a group
• Create and modify computer accounts
• Create, enable and unlock user accounts
Audit
• Change the system audit policy
• Change settings audit of an object
• Audit policy change by the user
Services
• Create or exit a process
• Initialize an application
• Create or modify scheduled tasks
• Change firewall settings
Objects
• Indirect object access request
• Change object permissions
• Delete objects
• Modify registry values

Figure 5-8. Windows Event Log Contents[165]

The detailed categories for Windows Event Logs include:

- **Application Log** - Application logs contain events that are logged by a program or application. Events such as application backup failures and antivirus malware detections can be found in the Application log. Application logging is controlled by each individual program and not every application will generate events. An investigator reviewing application logs should review what types of activities are being logged as well as which might be deemed suspicious.

- **System Log** - System logs contain events that are logged by Windows Operating System services. Events such as system startup and shutdown and time changes are recorded in System Logs. Device Driver activities can also be found within System Event Log files.

- **Security Log** - Security Event Logs contain audit information pertaining to key actions of the system, including applications services and related user activities. These events might include account logoff and logon events, account escalation events, and other privileged access requests. These audit logs are outlined as either an “Audit Success” or “Audit Failure”.

- **Setup Log** - Setup logs contain information about the installation of the operating system.

Application Type and Services Logs are a newer category of event logs collected in Windows.

[165] http://www.thinkmind.org/index.php?view=article&articleid=icimp_2016_2_20_30032

The presence of these logs will only be found on systems running Windows 7™ or later. These logs give higher levels of granularity on actions occurring on the system. Any application can have an associated log file created with these utilities. While there are several other event logs sources being collected, the primary categories are:

- **Admin** - Admin Event Logs are primarily recorded for administrators and support personnel. These logged events are specifically meant to identify if an application or service is functioning properly.

- **Operational** - Operational events are commonly used for analyzing or diagnosing an issue or occurrence. Certain events within the operational log that might be of value include the addition or removal of hardware from a system.

- **Analytic** - Analytic logs are commonly used to provide status updates via event logging to monitor the progress of an application. Certain issues will be logged in Analytic logs which might indicate an issue with the development of an application or a bug.

- **Debug** - Debug logs typically contain verbose activity logs of actions related to a system procedural attempt to isolate an issue for troubleshooting.

Logon Types found within the Security Event Log

Windows Logon events are one of the most commonly reviewed sources of evidence in the Security Event Log. An investigator should understand the differences in Logon Types to ensure evidence is properly interpreted. Each Logon event will include details that list the "Logon Type" for the event. It is important to understand each of these actions to properly reconstruct system activity.

- **Logon Type 2: Interactive** - An interactive logon event is triggered when a user attempts to logon via console access to the system. This commonly occurs when a user physically uses the system' s local keyboard and mouse to authenticate.

- **Logon Type 3: Network** - A network logon event is recorded when a user accesses a system via network authentication. This most commonly occurs when a user is accessing a file share or shared printer on the target system. Network services authentication may also use this type of logon.

- **Logon Type 4: Batch** - These events are recorded when a scheduled task is executed using stored credentials. Other scheduled jobs might also be recorded as a Logon Type 4.

- **Logon Type 5: Service** - The execution of a script or process utilizing a service account is recorded as a Logon Type 5.

- **Logon Type 7: Unlock** - Unlock events are created when a user returns to a system and unlocks it via keyboard and mouse. This will only be triggered if the lock screen setting is enabled on the target system.

- **Logon Type 8: NetworkClearText** - This event is similar to Logon Type 3; however, this event occurs when the password to the user account was sent in clear text. This is also used for Internet Information Services interactive logins or unencrypted (clear-text) logins to applications.

- **Logon Type 9: NewCredentials** - The NewCredentials Logon Type is associated with a user impersonating another account. Typically, this occurs when scheduled tasks or processes are launched with the "Run As" command.

- **Logon Type 10: RemoteInteractive** - The RemoteInteractive Logon Type is associated with access to a system via Remote Desktop using "RDP" services. VNC and similar applications instead utilize Type 3.

- **Logon Type 11: CachedInteractive** - This event is recorded when a user is authenticated in the domain using cached credentials. The most common scenario for this is when a system does not have access to the domain servers - the user is then authenticated against cached credentials stored on the system.

●Log Source Identification

At the foundation of almost every operating system, an auditing and logging system can be found. For example, and as described above, Microsoft Windows-based hosts have comprehensive event logging functionality that can be a highly valuable source of evidence when reviewing activities and building an incident timeline. Event logs can help answer questions pertaining to the activities of a user account and operational information on most applications, as well as assist in identifying logon and logoff activities and other potentially suspicious actions.

●Local and Centralized Log Storage

With almost every application creating some type of log, vast storage and infrastructure must be in place to properly store and provide secured access to logs. Understanding an organization' s logging architecture and policies is a very important aspect to determining sources of evidence.

There are two main methods for log storage:

- **Local Log Storage** refers to when any and all logs from a system are stored locally on the same system. While this can be effective, an investigation requiring logs from dozens or even hundreds of systems could be severely delayed in the log retrieval process due to the complexity of organizing access to all related sources. When considering evidence collection methods, care should be taken concerning the amount of effort required to collect the log files for analysis. It may be useful to automate the collection of these logs to reduce resources requirements.

- **Centralized Logging** is another means of configuring log storage. After the log file is created on the local file system, the log file is transported to a log collector for storage on a centralized logging server. This can be especially useful when trying to aggregate a series of logs from multiple systems.

●Log Retention

Another important consideration when identifying potential evidence sources is clarifying the retention period on the logging infrastructure. It is far too common for an investigator to attempt to review a log source only to find that the logs do not go back far enough in time, or that logs of interest are no longer available on the system. An experienced investigator will attempt to determine the retention period on available logs as early as possible in an investigation.

Size constraints are usually a key decision-making factor when an organization decides how long to store logs. An organization with several thousand hosts may not have the storage capacity to retain logs for longer than deemed functionally necessary. Other considerations should be reviewed as well, including any compliance requirements for logging such as regulatory records retention. Some regulated organizations are required to store their logs for a certain period of time. This information can be leveraged to identify if there are gaps in their logging infrastructure which might indicate policy violations or evidence destruction.

●Log Tampering

A key issue with standard logging is that it can be quite difficult to identify whether logs have been altered or deleted. Both scenarios must always be taken into consideration, as they could directly impact the outcome of an investigation. Log tampering involves the deliberate or accidental alteration of any log files or records within an investigation.

To protect against log tampering, safeguards have been created to identify these actions. Permissions-based restrictions are implemented in Microsoft Windows to prevent a user from deleting the event log entirely. Users will still have options to clear the log, but that action itself creates a new log entry detailing the activity. These logs can be a very important source of evidence in an investigation.

However, there are still many vulnerabilities that allow a user to gain the highest level of privileges on a system (SYSTEM or “root”). In certain cases, users can modify and delete log entries either in an individual record-by-record manner or by removing the log entirely. Certain malware types also utilize these techniques as part of an anti-forensics mechanism to avoid detection.

Another protection mechanism is implemented by many organizations that utilize centralized logging capabilities. In systems using centralized logging, specified log files are not stored locally on the system and are typically sent via network connection to a remote logging server. Alerts can be configured when a log source halts log forwarding or if tampering is suspected. Some centralized logging applications allow for cryptographic hashing of log files both at transmission and after storage to ensure logs have not been modified. An experienced investigator will take all of these points into consideration when deciding which questions to ask regarding the availability of event, application or system logs.

●Logging Levels

Most logging frameworks support several logging profiles, allowing the system owner to configure key characteristics of the logging system. Most logging levels allow customization of how much data is recorded in each log and often which events will be recorded. Though not every application utilizes these main logging levels, most will have a similar logging structure. By understanding the difference in logging levels, an investigator can prioritize what types of information to review first.

- **Debug** - Debug is typically the most verbose logging level. It is designed to record as much detail as possible for identifying and troubleshooting issues. A log that is set to debug might contain additional information including API keys, access tokens, and other application sensitive information.

- **Information** - The information log level is commonly used to output details that might be useful in the day-to-day operation of an application. These logs usually display the progress of an application in specific (high) detail.

- **Warning** - Warning log levels are often used to handle system or application exceptions and other key logging events. A warning event might trigger when a configuration file is not present or for other important but not fatal errors.

- **Error** - Error log levels are used to log any unhandled exceptions. This would include any errors or unexpected behavior while an application is running.

- **Fatal** - Fatal levels are specifically used for exceptions that trigger a FATAL exception in an application. These logs are used to quickly identify issues with an application or what might have caused it to crash or not launch.

●Advanced Correlation with SIEM technology

A Security Incident and Event Management (“SIEM”) system is an application or appliance that correlates events from corresponding systems’ log data and other sources to identify potential security risks. SIEM technology typically combines log management and data aggregation with real time monitoring and alerting. These capabilities provide advanced detection mechanisms that can be utilized to identify risk activities within a network, in a semi-automated fashion. Event correlations are available within a SIEM dashboard, making it easier to identify systems or activities of interest for investigators.

●Server and System Logging

Most applications and services provide at least a basic level of logging capabilities which can be used as evidence in an investigation. Services such as “Active Directory” (AD), DNS, and VPN might contain crucial sources of evidence that should be considered in the scope of an investigation. Much like other artifacts, these services and applications must be configured for adequate logging. Depending on the settings, logging might be too minimal to provide context or may be overly-verbose and cause fatigue during the analysis phase.

●Active Directory

Active Directory is a domain-based network service that automates the management of user information, security policies, and access to distributed resources across an organization. Active Directory logs contain detailed records and relate to host artifacts of interest that can assist in the identification of user and host based activities. Since Active Directory is commonplace across most organizations, these sources of evidence can be very helpful. There are several particularly useful artifacts to review from Active Directory.

The "NTDS.DIT" file[166] on the Active Directory Server contains details about an organization. This includes information about every user, such as the time of last account login as well as a series of flags that can be set on the "UserAccountControl" Field. An overview of key items of interest is outlined below:

- **SCRIPT** - This lists the logon script (if any) to be run at the time of a user logon event.

- **ACCOUNTDISABLE** - If this flag is set, the user account is listed as disabled in Active Directory.

- **PASSWD_NOTREQD** - Accounts with this setting will not be required to have a password associated with their account.

- **PASSWD_CANT_CHANGE** - The user will not be able to change their account password.

- **INTERDOMAIN_TRUST_ACCOUNT** - This will detail domain trust permissions for other domains.

- **SERVER_TRUST_ACCOUNT** - This is a computer account associated with a domain controller that is a member of the same domain.

The NTDS.DIT file also contains password hashes (both LM and NT) for each user in encrypted format[167]. The settings and configuration of Active Directory may include key pieces of information that could be utilized by an investigator to identify suspicious activity or privilege escalation.

●DNS Logging

DNS queries can be another vital source of information during an investigation. Unfortunately, due to the size and volume of DNS logs, most organizations choose to not record DNS requests. If available, these records can identify many types of suspicious activity. Below are some of the capabilities DNS logging enables, to show the relative value they hold as sources of evidence:

- **Indicator of Compromise** - DNS resolution requests can be (automatically or manually) related to OSINT and PROPINT sources to identify matches with known C&C.

- **Intelligence Mining** - Based upon similarities in registration details, such as Fully Qualified or Top Level Domain Names (FQDN or TLD) or registrant identity and related metadata, intelligence

[166] https://technet.microsoft.com/en-us/library/cc961761.aspx
[167] http://ntdsxtract.com/downloads/ntdsxtract/ntds_forensics.pdf

that may lead to additional C&C can be discovered.

- **Sinkholes**[168] - If (or as) malicious DNS are discovered, the FQDN or TLD can be configured in DNS Sinkholes to assist investigators with the discovery of infected hosts, and to capture PCAPs for analysis of cybercrime communications and related activities.

●Password and Certificate Management

Often referred to as "the keys to the kingdom", password and certificate management servers are highly sensitive in nature. Unauthorized access to the information stored on these systems could lead to a much larger incident, particularly in organizations with shared (protected) resources and infrastructures such as partner networks or vendor/service provider client support networks. One benefit of these types of technology is that there are typically heavily embedded auditing and reporting capabilities built into the systems and related processes[169]. An investigator should request any available logs and audit records or reports from a password or certificate management server and review them as potential sources of evidence.

●VPN Logging

While there are many VPN technologies and providers, VPN logs can be an excellent source of information for an investigation. Cybercriminals often obtain user credentials and attempt to gain access via an organization' s VPN services. By analyzing available VPN logs, investigators can correlate that information with a user' s activity from artifacts on endpoint hosts or other services logging sources. Analysis of these sources can provide several artifacts of interest. For example, it is possible to identify outliers if geolocation techniques are applied to each source IP address. If a user normally logs into their corporate VPN from a home location and the user account is seen logging in from overseas at odd hours of the night, it might be a strong indicator that the user's credentials have been compromised.

●Physical Security and Monitoring

Physical security monitoring logs are another potential source of evidence that must be considered by an investigator. Proper access controls help prevent unauthorized access to facilities and equipment. The ability to review logs and evidence of physical access and related activities can be significant in an investigation.

- **Access Control Systems** - It is important to define who has access to a physical location or restricted area. By default, access should be denied to anyone who does not have proper credentials to enter a controlled area. Physical barriers and badge access control systems often have audit logs that can be reviewed by investigators to identify suspicious activity. These access logs can also assist in creating a profile of a suspect or group of individuals. An investigator might use these logs to review a user' s normal activity and identify anomalies.

[168] https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

[169] For example, Payment Card Industry vendor/client compliance requirements: https://www.pcisecuritystandards.org/pci_security/

- **Fire and Safety** - The best time to commit a crime is usually when law enforcement or emergency response personnel are otherwise occupied. When cybercrimes are committed, it can be useful to determine if any fire or safety systems logs indicate coincidental responder service notifications.

- **Audio and Video Monitoring** - Surveillance cameras or CCTV and other audio/video monitoring systems can provide useful sources of evidence in cybercrimes involving malicious insiders.

Chapter 5: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

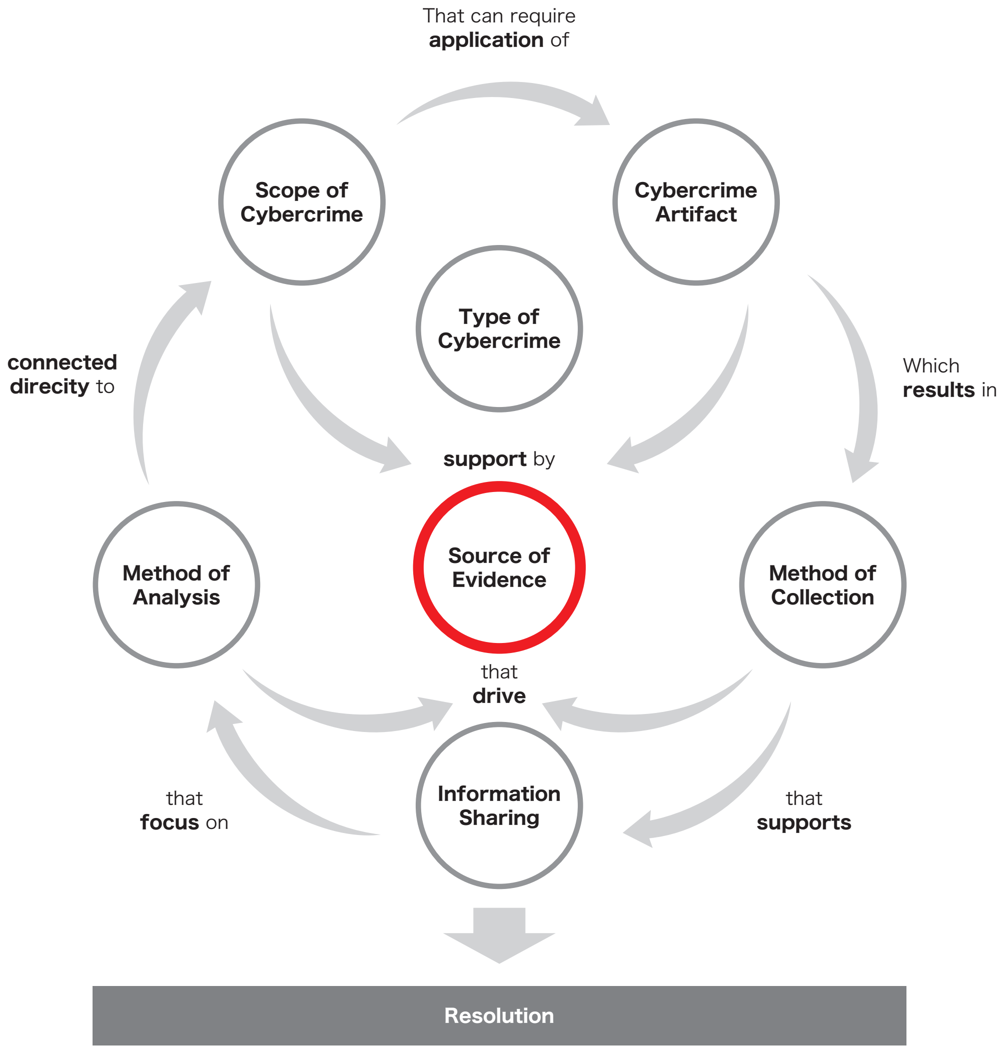


Figure 5-9. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 5-10. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 5-11. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

<legend> S : Strategic T : Tactical P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a strategic knowledge of the sources of evidence available to determine cybercrime objectives and profiles of related organizations.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial tactical source of information for identifying, developing, monitoring, and collecting sources of evidence related to cybercrimes.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. The type(s) of cybercrime will be determined by evidence. Investigators must have a tactical understanding of the indicators and artifacts that can be discovered from sources of evidence to determine cybercriminal activities and objectives.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well as information sharing according to the type of cybercrime committed. Judiciary personnel should have a tactical understanding of the sources of evidence useful to defining cybercrimes.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The type of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts. They will assist with collection and analysis of sources of evidence.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 5: Review

1. What sources of evidence exist to identify cybercrime?

   Answer: External and Internal.

   Examples: HUMINT/ELINT, Computers, Servers, Mobile Devices, PBX Systems, etc.

2. Where can such evidence be found externally and internally to an organization?

   Answer: Threat Intelligence Sources, Hacker Forums, Botnet Control Panels, Networks, Hosts, Service Logs

   Examples: OSINT/PROPINT/RUMINT, SIEM, Metadata, Registry Settings, VPN Logs

3. How do evidence sources differ in content, reliability, and structure?

   Answer: Structured vs. Unstructured, and Volatile vs. Persistent.

   Examples: Logs vs Process Memory details

Case Study 5: Analyzing the Mirai Botnet Using Forensic Techniques

- **Crime**: Unauthorized Access, Business Interruption
- **Suspect(s)**: Botmasters
- **Means**: Malware & Botnet Development, Credential Abuse
- **Motive**: Botnet As A Service reputation and financial gains

The Mirai botnet, responsible for some of the most disruptive distributed denial-of-service (DDoS) attacks in recent history, serves as a notable case study for understanding the application of forensic techniques in cybercrime investigations.

The Mirai botnet's sophisticated attack mechanisms had a significant impact on various high-profile targets. Among the notable victims was Dyn, a major DNS provider. The attack on Dyn in October 2016 disrupted services for numerous prominent websites, including Twitter, Reddit, Netflix, and Spotify, leading to widespread internet outages across the United States and Europe. Another key victim was OVH, a leading French web hosting service provider, which faced a barrage of traffic that peaked at over 1 terabit per second. Additionally, the Krebs on Security blog, operated by cybersecurity journalist Brian Krebs, experienced one of the largest DDoS attacks ever recorded, compelling network providers to revise their security protocols and reevaluate their defenses.

A 2016 study by cyber security company Imperva[170] related to these events depicted the global nature of infected iOT devices leveraged by the Mirai botnet. It is depicted in the following diagram.

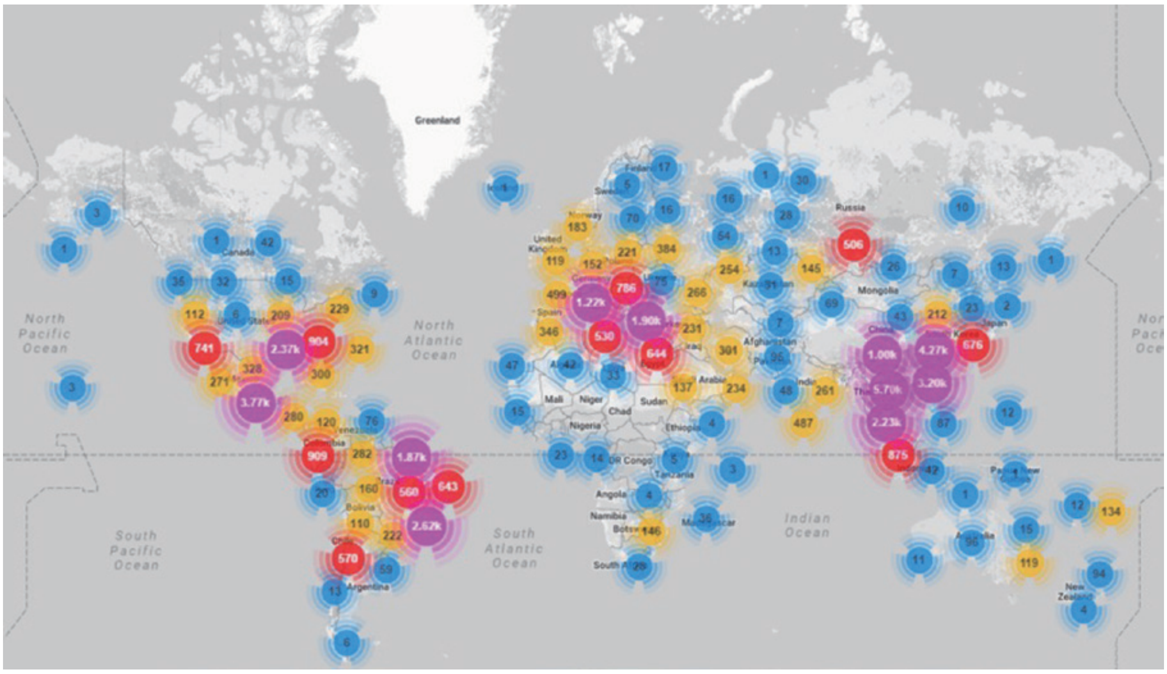


Figure 5-12. Mirai botnet

What makes Mirai particularly insidious is its method of infiltrating IoT devices by exploiting default login credentials, converting them into zombies to orchestrate large-scale attacks. The Mirai

[170] Source: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

botnet operates by infecting Internet of Things (IoT) devices, a category comprising everyday objects such as cameras, routers, and DVRs that are connected to the internet[171]. Mirai utilizes a brute-force attack method to gain control over these devices. By scanning for IoT devices that still have their default factory login credentials, Mirai can easily infiltrate them. Once infected, the compromised devices, also known as "bots," are controlled by a command-and-control server operated by the botnet author.

The topology of a Mirai botnet and its overall scope is shown in the following figures[172]:

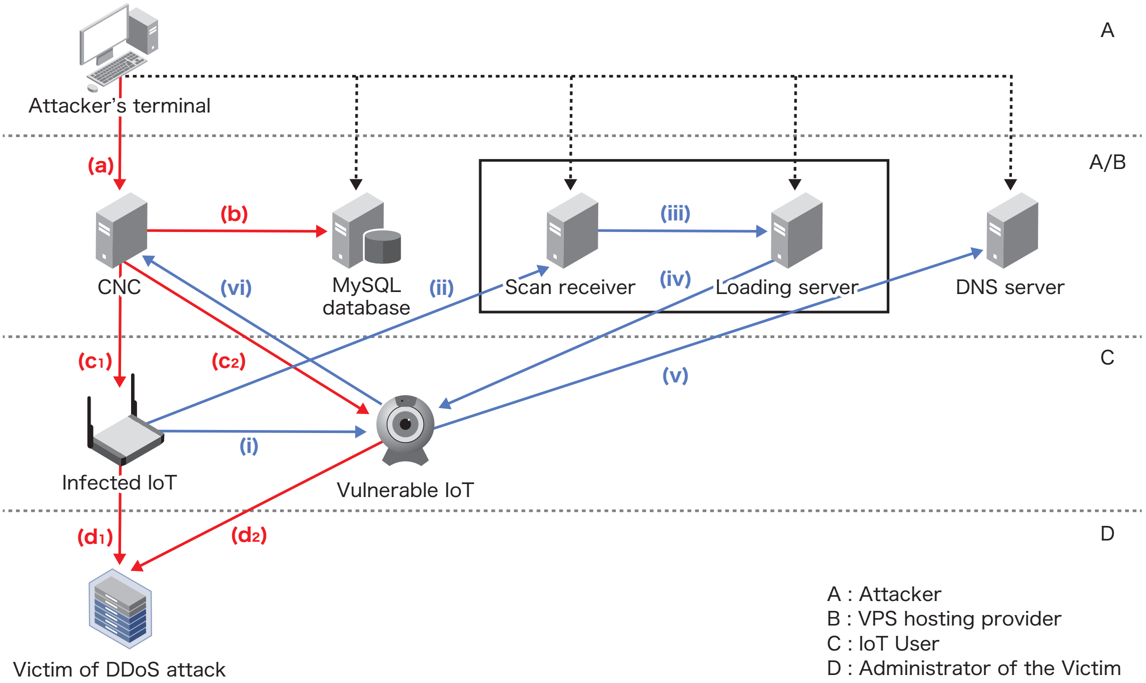


Figure 5-13. Mirai botnet topology

[171] https://storage.googleapis.com/gweb-research2023-media/pubtools/3982.pdf

[172] https://www.sciencedirect.com/science/article/pii/S2666281720300214?via%3Dihub

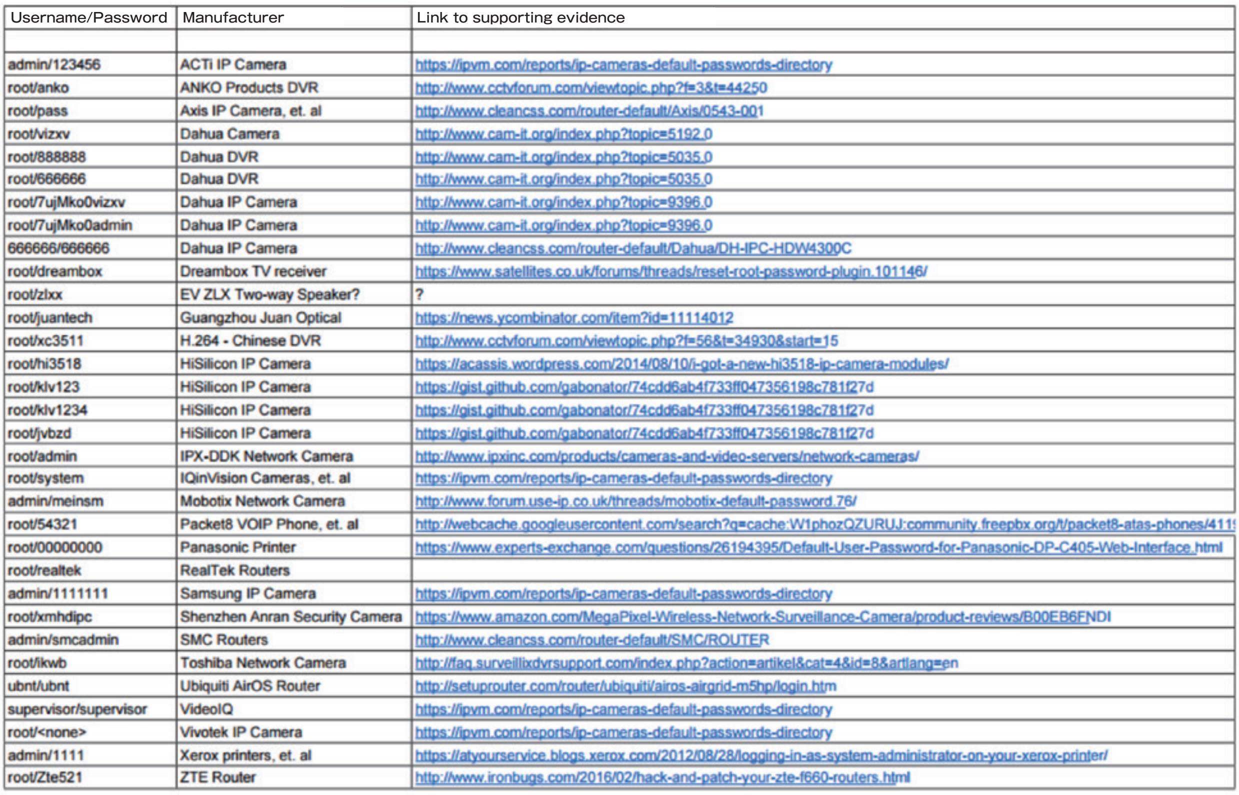
Figure 5-14. Top Mirai-Compromised Device Vendors

CWMP(28.30%)		Telnet(26.44%)		HTTPS(19.13%)		FTP (17.82%)		SSH(8.31%)	
Huawei	3.6%	Dahua	9.1%	Dahua	3.4%	D-Link	37.9%	MikroTik	3.4%
ZTE	1.0%	ZTE	6.7%	MultiTech	26.8%	MikroTik	2.5%		
		Phicomm	1.2%	ZTE	4.3%	ipTIME	1.3%		
				ZyXEL	2.9%				
				Huawei	1.6%				
Other	2.3%	Other	3.3%	Other	7.3%	Other	3.8%	Other	1.8%
Unknown	93.1%	Unknown	79.6%	Unknown	20.6%	Unknown	54.8%	Unknown	94.8%

Figure 5-15. Top Mirai-Compromised Mirai Device Types

CWMP(28.30%)		Telnet(26.44%)		HTTPS(19.13%)		FTP (17.82%)		SSH(8.31%)	
Router	4.7%	Router	17.4%	Camera/DVR	36.8%	Router	49.5%	Router	4.0%
		Camera/DVR	9.4%	Router	6.3%	Storage	1.0%	Storage	0.2%
				Storage	0.2%	Camera/DVR	0.4%	Firewall	0.2%
				Firewall	0.1%	Media	0.1%	Security	0.1%
Other	0.0%	Other	0.1%	Other	0.2%	Other	0.0%	Other	0.0%
Unknown	95.3%	Unknown	73.1%	Unknown	56.4%	Unknown	49.0%	Unknown	95.6%

Figure 5-16. Examples of Default Login Credentials in Mirai-Compromised Devices[173]:



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

A distinct technical aspect of Mirai is its use of a domain name generation algorithm (DGA), which periodically generates multiple domain names for the command-and-control server, making it challenging to disrupt the botnet's communication with its bots. Additionally, the botnet employs

[173] https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

various types of DDoS attack vectors, including UDP floods, TCP ACK floods, and HTTP POST attacks, to overwhelm network resources and incapacitate target services. These vectors are specifically chosen based on the vulnerabilities of the targeted systems, maximizing the impact and disruption caused by the attack. Mirai also employs a modular architecture, which allows for the rapid incorporation of new features and attack capabilities. This modularity ensures that the botnet can adapt to evolving security measures and continue its malicious operations effectively.

Brian Krebs, a well known cybercrime researcher, conducted an investigation following the 2016 Mirai botnet attacks. He identified several individuals[174] whom US authorities subsequently detained and prosecuted as creators of Mirai. Notably, each was a US citizen who avoided jail time by cooperating with authorities, and they were sentenced to 5 years probation and ordered to pay for related financial damages[175].

Unfortunately, the release of the Mirai source code on GitHub resulted in the production of several later varints including "OMG", "ZHtrap", and "Mukashi"[176].

Forensic Analysis of Mirai Botnet

To understand the construction and operation of the Mirai botnet it is necessary to understand the topology of the Mirai botnet, then to gather sufficient operational intelligence from compromised devices. It is also important to gather evidence from multiple sources from each device in order to associate real from "false-flag" settings. Sometimes, especially in iOT environments, such evidence is difficult to obtain after-the-fact, and instead a laboratory analysis must be conducted and the results used to develop network and operating process detection signatures.

A detailed example of laboratory forensic procedures is provided by a study conducted in 2020[177].

[174] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
[175] https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/
[176] https://heimdalsecurity.com/blog/mirai-botnet-phenomenon/
[177] https://www.sciencedirect.com/science/article/pii/S2666281720300214

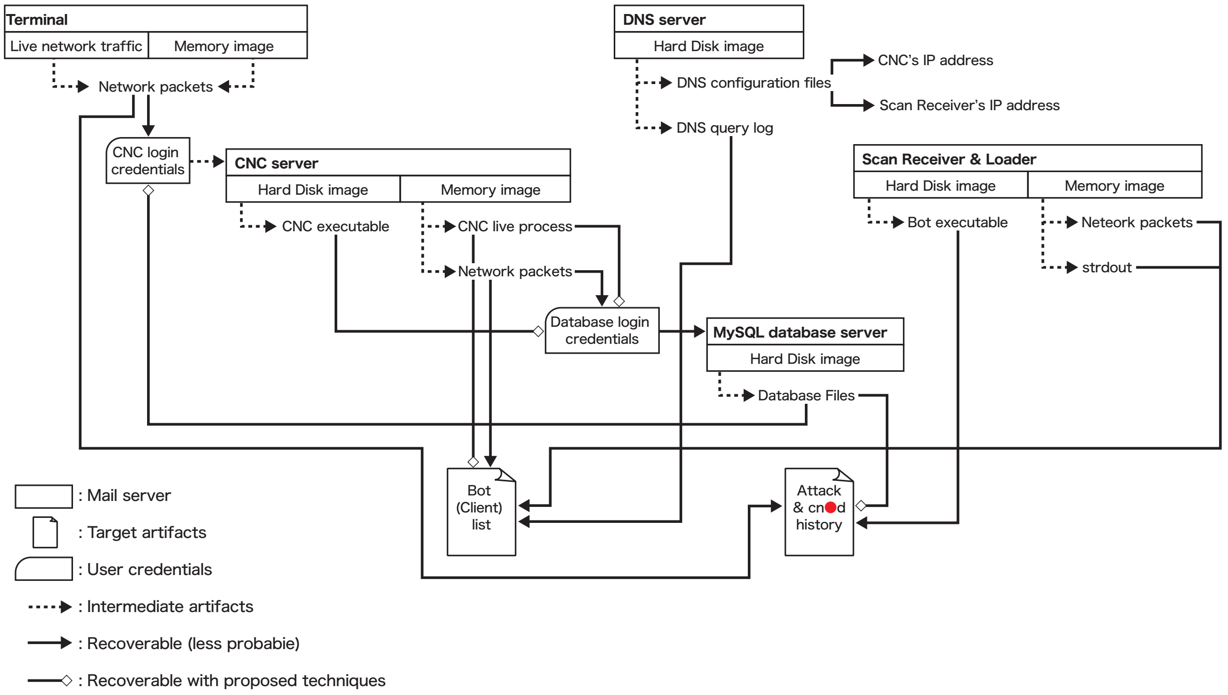


Figure 5-17. Example of laboratory forensic procedures

Crucially, in that study it was discovered that forensic acquisition of several stages of the Mirai botnet were required to gain comprehension of the botnet's distributed architecture. Common aspects of the forensic procedures included live memory and network communications acquisition, binary reverse engineering, and process and communications analysis from each compromised device. In particular the analysis of process memory to yield communications configuration was important.

Findings and Implications

The forensic investigation of the Mirai botnet as outlined in the referenced articles revealed significant insights into its modus operandi. This included a deeper understanding of its propagation mechanism, attack vectors, and C2 communication strategies. The forensic analysis of the Mirai botnet underscores the necessity of employing advanced and multi-faceted investigative techniques involving multiple and disparate but linked sources of evidence including live network traffic, memory dumps, and binary reverse engineering - as well as source code analysis of public releases. Such information is invaluable for developing mitigation strategies, enhancing IoT security protocols, and informing regulatory policies.

Chapter 6

Methods of Evidence Collection

Introduction

The collection of digital evidence from its source is no less important than the analysis of the evidence itself. Often, the evidence collection process is subject to a high degree of scrutiny, with history providing many examples of prosecutions that have failed due to improper evidence collection or handling. Several factors including a crime' s nature, an investigator' s scope, human failure (on the part of an investigator or security team) to identify or recognize sources, and the technology used to access various types of data will determine what evidence can be acquired from the sources available. It is important to note that the ongoing proliferation of interconnected devices, cloud services, and auto-synced accounts can offer an investigator several sources from which to collect evidence.

Prior chapters have discussed the proliferation of computing and communicating devices across the "Internet of Things" and the expansion of traditional enterprise networks to include industrial and other functional operating systems. As previously discussed, the growth and adoption of cloud IAAS/PAAS/SAAS has also required additional considerations of sources of evidence in assessing the scope, nature, and objective of cybercrimes.

As the scale of evidence sources has dramatically expanded, so too has the need for automation to collect and preserve evidence required to evaluate and prove cybercrimes.

This chapter will examine automated and manual methods of evidence collection. The chapter will then discuss differences in evidence collection based on the type of cybercrime being investigated. Additionally, this chapter will provide investigators with a reference framework for developing effective methods of evidence collection and assist organizational managers in defining policies, systems, and procedures for defense and protection.

At the conclusion of this chapter, readers will understand:

- How can evidence of cybercrime be collected?
- How should evidence be collected?
- What measures or steps should be taken to ensure reliability of evidence?
- How do evidence and related methods differ by type of cybercrime?

Topic in Artifacts of Cybercrime

Figure 6-1. displays topic categories in the “Methods of Evidence Collection” knowledge domain.

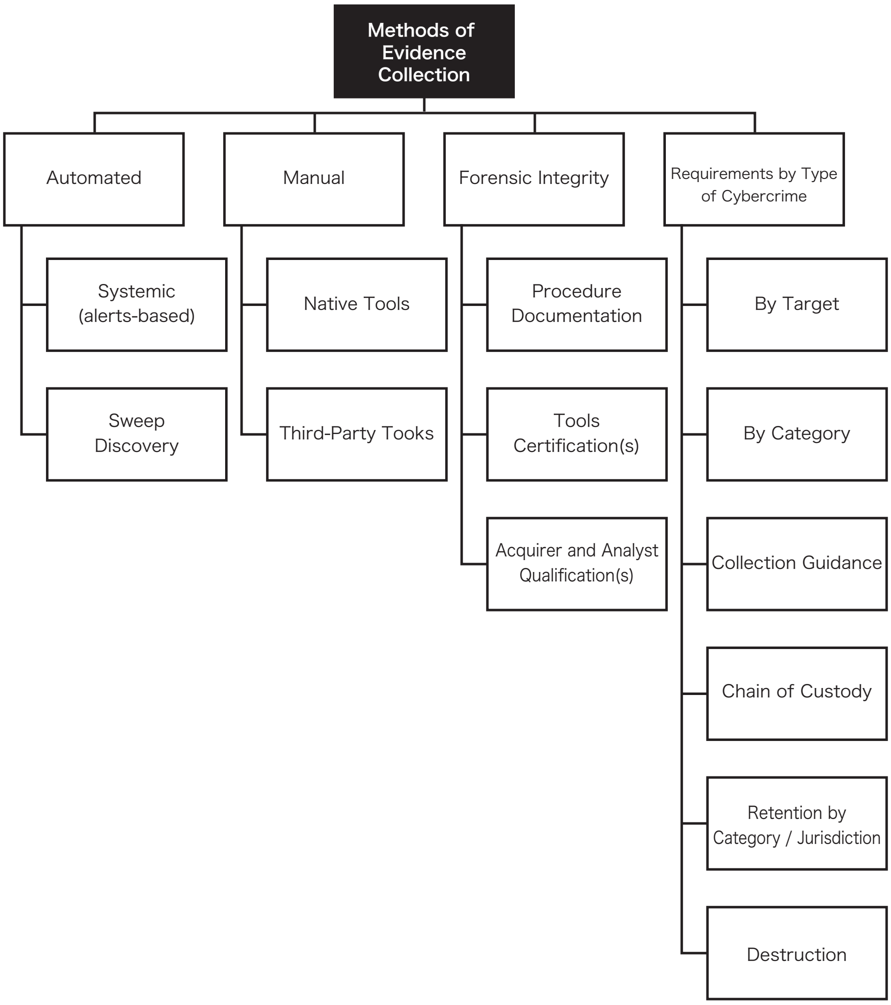


Figure 6-1. Topic Categories in the “Sources of Evidence” knowledge domain

What are Methods of Evidence Collection?

Today, there are several methods of collecting evidence from digital sources that enable an investigator to determine a cybercrime's scope, objectives, and TTPs. Historically, investigators in a network security role have focused on sources of evidence related to specific systems that propagate IOC alerts. Investigators have then identified other associated "systems of interest" to examine for corollary evidence, although occasionally important data or artifacts are misunderstood and lead to conclusions based upon partial information. Evidence collection practices based upon IOC-following are sometimes referred to as a "ball-of-string", as you never know where the string will lead or how long it is. Consequently, the cost in resources (people, tools, time, and related financial costs) can be as long as the "ball-of-string". Complicating the matter, if investigators are able to finally unravel the "ball", they may find that a company's SIEM has already cycled out the data they were seeking.

A more efficient procedure is needed to determine the scope of a cybercrime. The effectiveness of the approach to investigate computers, interview personnel, and review log sources (i.e., sources of evidence described in Chapter 5) depends upon a scalable but comprehensive process of evidence collection. To facilitate this, a "triage" approach should be used. Triage-based evidence collection refers to the use of systems, tools, and collection activities in a phased approach to more quickly identify the type and location of evidence. This provides an understanding of the volume, complexity, and scope of the evidence and overall investigation. Such evidence is derived from artifacts and data based on both intelligence and investigative sources. Intelligence sources may include conducting interviews as well as reviewing "Open Source" and "Proprietary" information published by law enforcement (or peer companies) or produced by information security researchers and analysts.

It is important for investigators to be able to explain that they have not only identified and preserved relevant sources of technical evidence related to the investigation, but also that any sources determined to be irrelevant were evaluated based on a defensible analysis process.

The process of triage-based evidence collection involves three phases to help an investigator (or auditor, as the process supports risk assessment and management objectives as well) identify the specific systems of interest from which to collect evidence:

1. **Sweep**: The triage process begins with an assessment of all managed (or accessible) hosts in the subject IT estate. This involves collecting data from endpoint hosts that can be correlated with network and security reporting (such as SIEM) logs. The first phase focuses the investigative efforts on "systems of interest".
2. **Investigate**: The second phase further reduces the investigation's scope by collecting metadata on the subset of data that requires deep technical analysis or collection to preserve specific evidence according to a policy or procedural mandate.
3. **Collect**: The process of triage evidence can be retrieved from many sources, but its utility to serve a particular objective depends on the reliability of the process of collection as well as the completeness of the information that the evidence is meant to convey through analysis.

Figure 6-2 below demonstrates the concept of a triage-based collection of evidence:

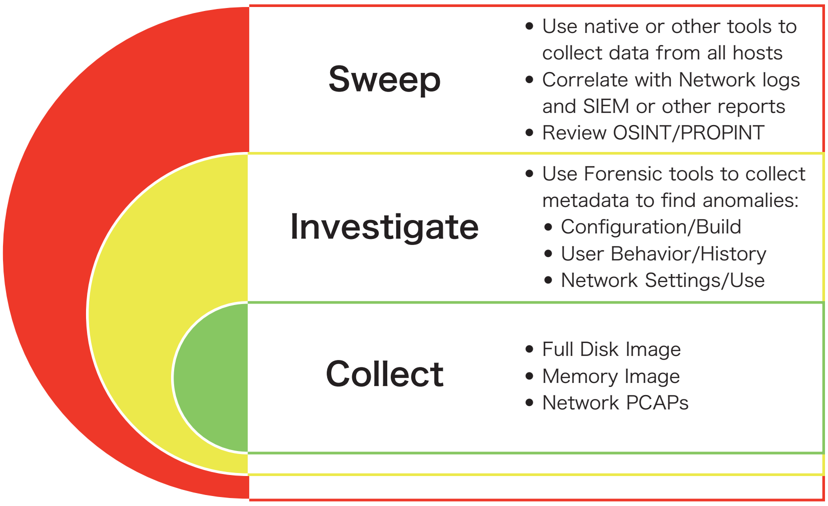

Sweep
• Use native or other tools to collect data from all hosts
• Correlate with Network logs and SIEM or other reports
• Review OSINT/PROPINT
Investigate
• Use Forensic tools to collect metadata to find anomalies:
• Configuration/Build
• User Behavior/History
• Network Settings/Use
Collect
• Full Disk Image
• Memory Image
• Network PCAPs

Figure 6-2. Triage-based Evidence Collection

This triage approach allows an investigator to collect data that can be interpreted in relation to an objective of a cybercrime. For example, if theft from a corporate account has occurred, this approach would allow the investigator to discern whether introduced tools (such as malware) were used on the involved systems and credentials.

The triage approach leverages automated and manual methods of evidence collection and is intended only as one suggested approach. For example, many organizations employ automation to reduce the burden of endpoint artifact discovery and evidence collection. In such cases, the following information may be more useful for understanding why such tools exist to support cybercrime investigations and the organization' s cyber security posture- as opposed to informing a collection method.[178]

In addition, it is worth noting that various professional practices and standards form methodologies "applicable to computer forensic investigations". These practices are generally accepted as:

- Identification of Evidence
- Evidence Collection and Acquisition
- Evidence Preservation and Assurance
- Evidence Processing
- Evidence Analysis
- Reporting

These practices are supported by national, international, and professional standards such as:

- ISO/IEC 27037[179]: "Guidelines for identification, collection, acquisition and preservation of digital evidence."
- ISO/IEC 27041[180]: "Guidance on assuring suitability and adequacy of incident investigative

[178] Please note that although certain artifacts and tools will be described, this chapter is intended only to demonstrate concepts and not to provide instruction or recommend tools for collection of evidence.
[179] https://www.iso.org/standard/44381.html. Published 2012 and last confirmed as current in 2018.
[180] https://www.iso.org/standard/44405.html. Published 2015 and last reviewed and confirmed as current in 2021.

method."

- **NIST SP 800-86**[181]: "Guide to Integrating Forensic Techniques into Incident Response."
- **SWGDE**[182]: "Scientific Working Group on Digital Evidence."
- **NIST CFTT**[183]: "Computer Forensics Tool Testing Program."

In all cases, investigators should review applicable standards and apply associated guidelines, practices, and procedures as required.

Automated Evidence Collection

Commercially available and open-source cybersecurity tools allow investigators to acquire data from a variety of sources, analyze the data, and determine its evidentiary value. Varied technologies collect artifacts according to indicators programmed to identify and highlight relevant artifacts by way of alerting mechanisms. Cybersecurity analysts and investigators can also use tools to automate otherwise manual methods of evidence collection.

Systemic (alerts-based logging)

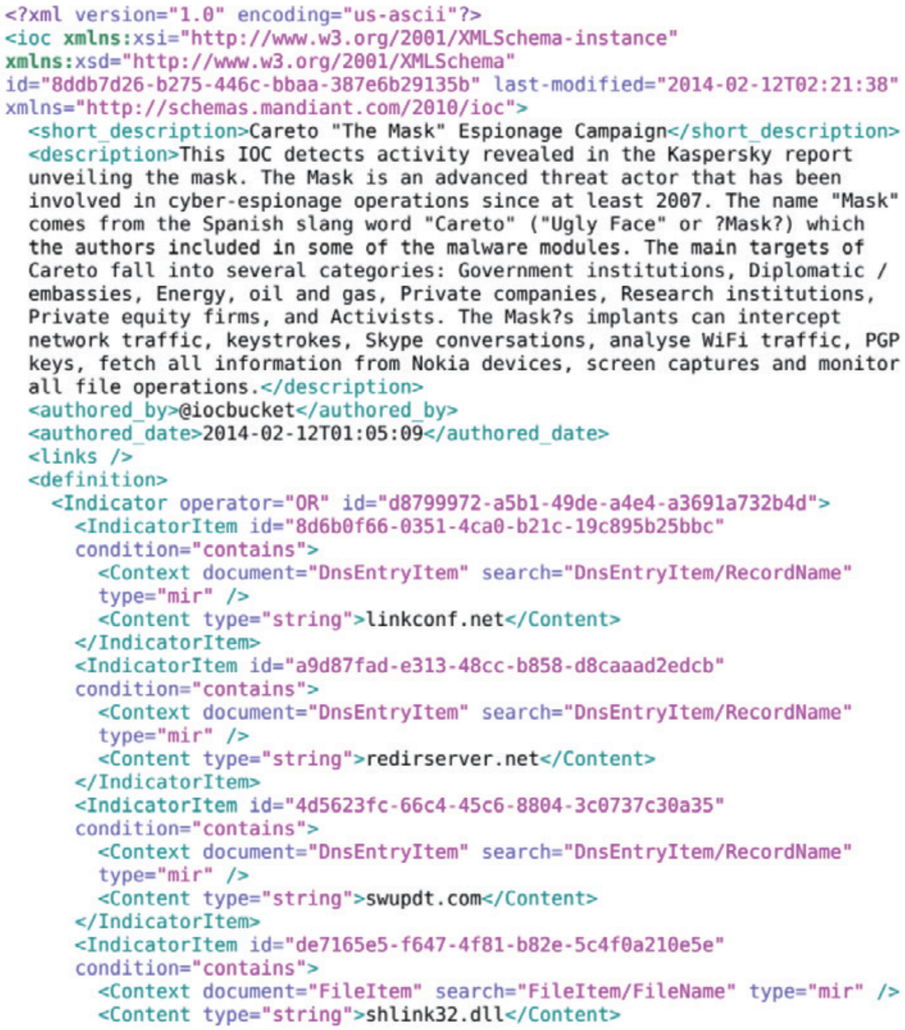
One essential technology that should be employed by organizations is an alerts-based system of logging indicators of compromise (IOCs). As described in Chapter 3, IOCs reflect artifacts such as date/time of events, pattern matches (cryptographic hash or heuristic behavioral signatures), and associated metadata that can provide useful details about a potential incident. The following example of an IOC refers to an alert condition for endpoint detection of "Careto" malware[184]:

[181] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf. Published 2006.

[182] https://www.swgde.org/documents/published-by-committee/forensics

[183] https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

[184] https://conf.splunk.com/session/2014/conf2014_FredWilmot_Splunk_Security.pdf



```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="8ddb7d26-b275-446c-bbaa-387e6b29135b" last-modified="2014-02-12T02:21:38"
xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Careto "The Mask" Espionage Campaign</short_description>
  <description>This IOC detects activity revealed in the Kaspersky report
  unveiling the mask. The Mask is an advanced threat actor that has been
  involved in cyber-espionage operations since at least 2007. The name "Mask"
  comes from the Spanish slang word "Careto" ("Ugly Face" or ?Mask?) which
  the authors included in some of the malware modules. The main targets of
  Careto fall into several categories: Government institutions, Diplomatic /
  embassies, Energy, oil and gas, Private companies, Research institutions,
  Private equity firms, and Activists. The Mask?s implants can intercept
  network traffic, keystrokes, Skype conversations, analyse WiFi traffic, PGP
  keys, fetch all information from Nokia devices, screen captures and monitor
  all file operations.</description>
  <authored_by>@iocbucket</authored_by>
  <authored_date>2014-02-12T01:05:09</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="d8799972-a5b1-49de-a4e4-a3691a732b4d">
      <IndicatorItem id="8d6b0f66-0351-4ca0-b21c-19c895b25bbc"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">linkconf.net</Content>
      </IndicatorItem>
      <IndicatorItem id="a9d87fad-e313-48cc-b858-d8caaad2edcb"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">redirserver.net</Content>
      </IndicatorItem>
      <IndicatorItem id="4d5623fc-66c4-45c6-8804-3c0737c30a35"
      condition="contains">
        <Context document="DnsEntryItem" search="DnsEntryItem/RecordName"
        type="mir" />
        <Content type="string">swupdt.com</Content>
      </IndicatorItem>
      <IndicatorItem id="de7165e5-f647-4f81-b82e-5c4f0a210e5e"
      condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">shlink32.dll</Content>
```

Figure 6-3. IOC Example for Systemic Alerting

Different products may use different IOC-modeling language, but each generally provides alerts on similar information. The most common IOC standards include Structured Threat Information eXpression (STIX)[185], Trusted Automated eXchange of Indicator Information (TAXII)[186], and “OpenIOC”[187]. Figure 6-4 demonstrates STIX alert architecture:

[185] https://stixproject.github.io/

[186] https://taxiiproject.github.io/

[187] http://www.openioc.org/

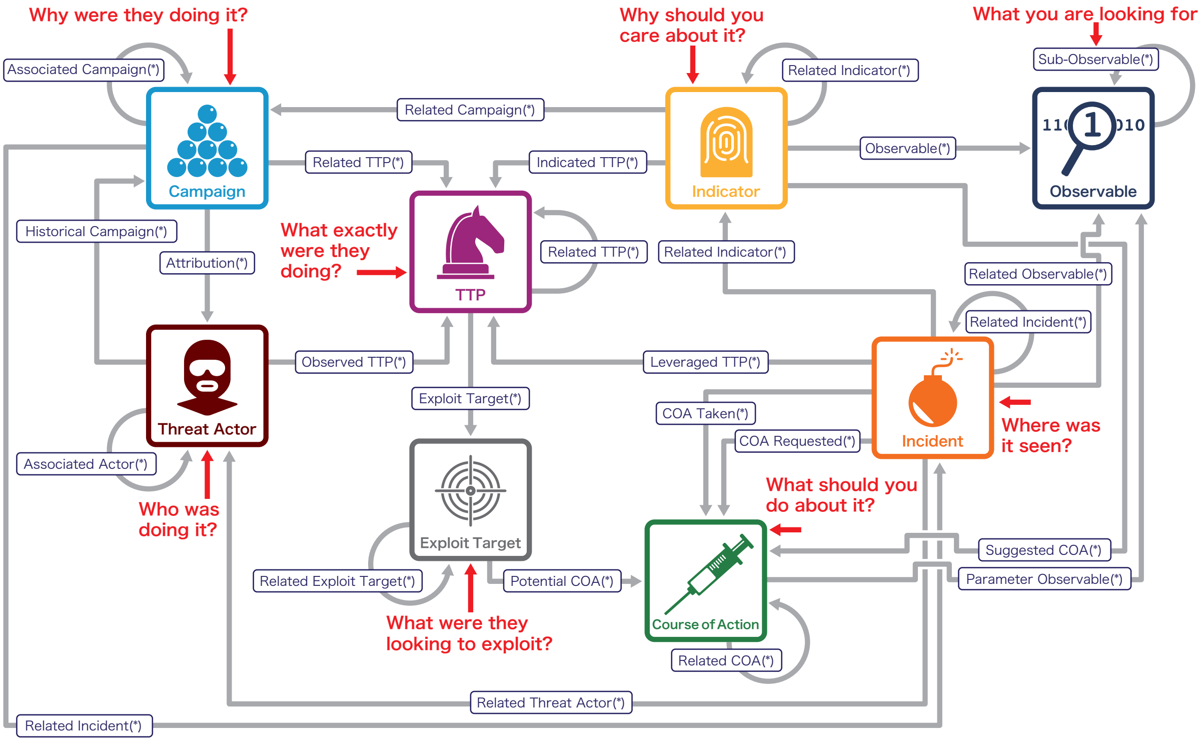
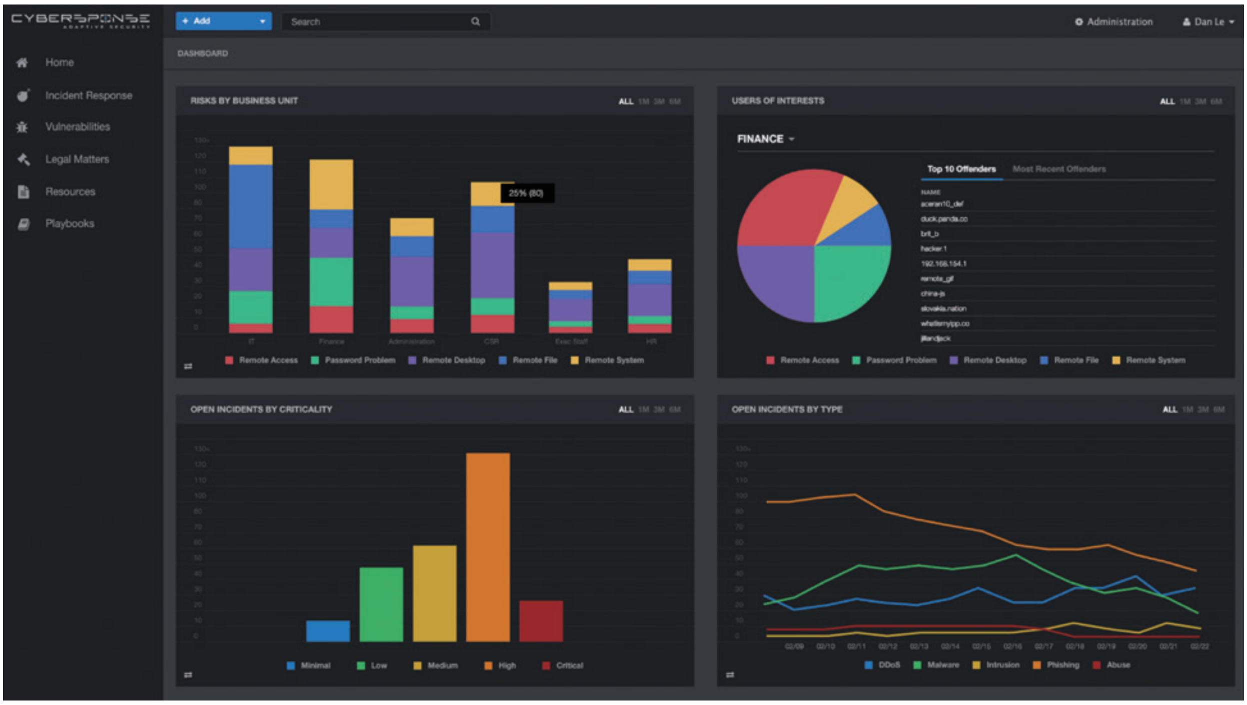


Figure 6-4. STIX Architecture of an Alert

These IOC standards were designed as a common interchange method for information sharing purposes. The commonality of the interchange format enables many cybersecurity and investigation products to systematically integrate threat intelligence to improve their independent (or interdependent, in some cases) detections of malicious activities in the environment that they monitor.

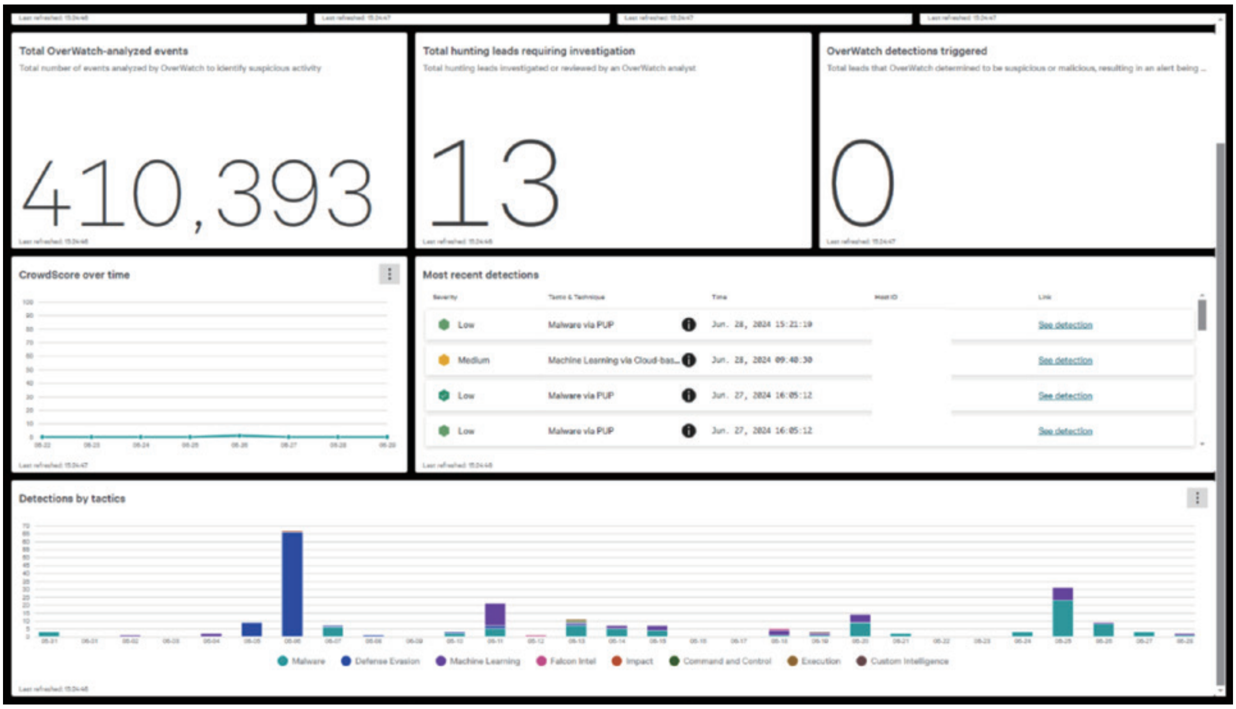
Some products still use proprietary protocols for information storage and exchange with limited “approved” partner solutions. However, even those products can often be synthesized into a common IOC format that enables a centralized/consolidated logging system to correlate IOC information and generate alerts. In those logging systems, profiles for logging contextual artifacts of cybercrime activities will be automated to support the systemic collection of evidence.

SIEM and similar consoles that converge data from monitored endpoints and sources of evidence can also be used for the systemic collection and analysis of evidence (to be discussed in Chapter 7). However, evidence collection requires context that may or may not be configured in standard products, and other workflow solutions have recently emerged to support cybersecurity, compliance, risk management, and cybercrime investigation requirements.



NAME
aceran10_def
duck.panda.co
brit_b
hacker.1
192.168.154.1
remote_gif
china-js
slovakia.nation
whatterrylpp.co
jillandjack

Figure 6-5a. Alerts-based Logging



Total OverWatch-analyzed events

Total number of events analyzed by OverWatch to identify suspicious activity

410,393

Total hunting leads requiring investigation

Total hunting leads investigated or reviewed by an OverWatch analyst

13

OverWatch detections triggered

Total leads that OverWatch determined to be suspicious or malicious, resulting in an alert being ...

0

Most recent detections

Severity	Tactic & Technique	Time	Host ID	Link
Low	Malware via PUP	Jun. 28, 2024 15:21:19		See detection
Medium	Machine Learning via Cloud-bas...	Jun. 28, 2024 09:40:30		See detection
Low	Malware via PUP	Jun. 27, 2024 16:05:12		See detection
Low	Malware via PUP	Jun. 27, 2024 16:05:12		See detection

Figure 6-5b. Crowdstrike Falcon Overwatch Alerts-based Logging

One important consideration for investigators is whether the information they are looking for is being logged. Another is whether the relevant system(s) have the reference point(s) of view to correctly correlate a given activity, given that modern network sensors often log network traffic while host sensors log host traffic- and investigators often need to correlate between the two data sources to properly identify a malicious event. Log fidelity is a byproduct of properly configuring logging systems and reviewing their output to ensure the accuracy and usefulness of stored logs in answering investigative questions and generating additional investigative leads. Investigators should determine what logging mechanisms are in place, what is being logged, where are those logs being stored, who has had access to those logs, and the retention policies of said logs. Before declaring that nothing is found in an investigation, these questions must be asked and answered by reviewing available logs. This is illustrated above in Figure 6-5 with "syslog" style messaging normalized from varied proprietary security products. When examining log files for events to base alerting systems on, or when performing actual collections to locate evidence, the question of how logging was configured should come first. Proof of log configurations should be included with collected evidence.

The effectiveness of alert-based logging is dependent upon a blend of qualified intelligence and audited systemic procedures. These must be managed to ensure that proper perspectives of the scope, type, and nature of evidence of cybercrimes are understood as they evolve with changing TTPs. An effective program will incorporate a balance between these perspectives and supporting automations. This helps an organization streamline an investigation and begin the process of recovery and resolution activities. Intelligence and information sharing has grown into an open-source, community-based platform with a widespread reach, augmented by some organizations offering a proprietary source for IOCs that assist in recognizing cybercrimes. However, as discussed in Chapter 4, IOCs are not "threat intelligence" until they are understood in the context of the risks to an organization.

"Sweep" discovery

An investigator must quickly determine the scope of a cybercrime to identify sources of evidence for preservation. In corporate environments, there may be a large and dispersed crime scene. Due to both the speed at which cybercrimes can propagate and the complexity of many computing environments, an initial triage phase of scanning or "sweep discovery" can assist the investigator.

The initial phase of scanning the estate is useful in enumerating a range of sources to identify where IOCs or other artifacts may exist. This helps the investigator focus collection and analysis activity on relevant systems first. The use of existing operating system and third-party software tools, scripts, and log files is common in conducting a sweep discovery. Often, this involves scanning an entire estate to identify sources of evidence that may have initially been considered irrelevant or unrelated.

A properly configured sweep discovery process will include data from several different sources including host-based (endpoint) and network (egress or other critical connections) monitoring. Some examples of host-based system sources include anti-virus logs, event logs, syslogs, and process monitoring logs. Other useful sources of information include configuration information (such as operating system and application versions), filesystem listings (complete or specific), user profiles and entitlements of use by system and applications, network configuration settings and host-based communicating services, persistent and scheduled services configurations, and shared resources connections. It is important to collect these artifacts in a forensically sound manner to ensure the reliability of evidence and to defend the process of the investigation if necessary.

Sweeps are often performed using popular forensic tools[188] such as EnCase™ and Access Data™ but they can also be executed with tools such as F-Response[189] or even free tools shared by the security community[190]. A sweep is simply intended to collect enough raw data to help an investigator

[188] https://www.guidancesoftware.com/ and http://accessdata.com/solutions/digital-forensics/ad-enterprise

[189] https://www.f-response.com

[190] https://github.com/AJMartel/IRTriage

identify evidence. As such, even the simplest operating system commands executed on endpoints and collected for extraction, transformation, and loading (ETL) can provide this type of data. Antivirus and endpoint configuration management software usually support the collection of data such as:

- Directory listings (DIR or lsof) of operating system and "user-space" files
- Network settings and configurations (NETSTAT or IP/ifconfig and ARP)
- Active Processes and their resources (TASKLIST or ps)
- Host configuration details (MSCONIFG or ls*)
- Event log details (WEVTUTIL or cat)

It can be helpful to think of the evidence collection process in terms of a funnel, where the top of the funnel represents the easiest data to collect (Sweep). As the funnel narrows, more effort is required to both collect and analyze the data (Investigate and Collect). Additionally, the fidelity (completeness and context) of data increases as the funnel narrows, which allows for a more thorough investigation. This phased approach is depicted in the figure 6-6 below:

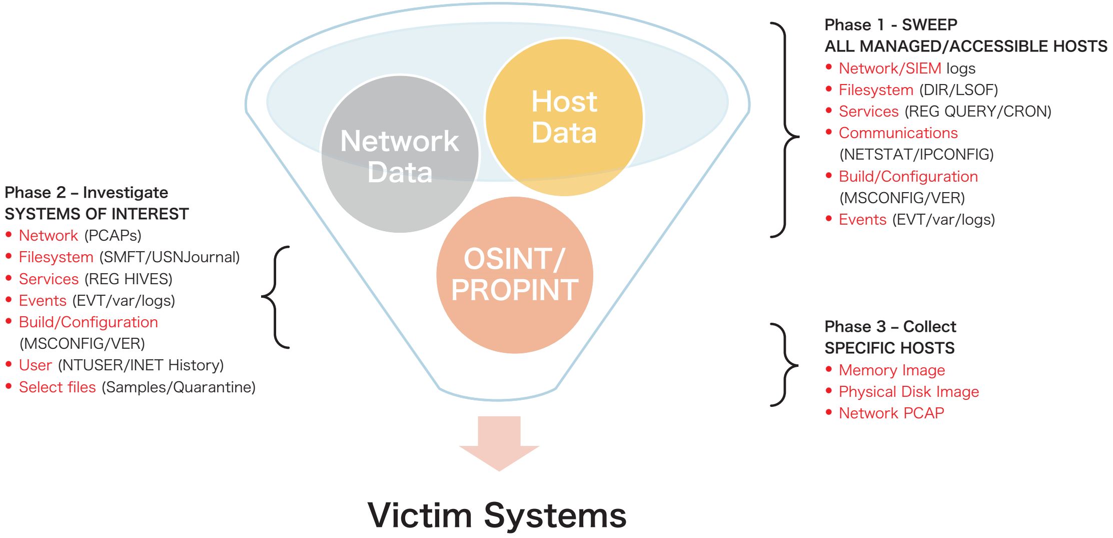


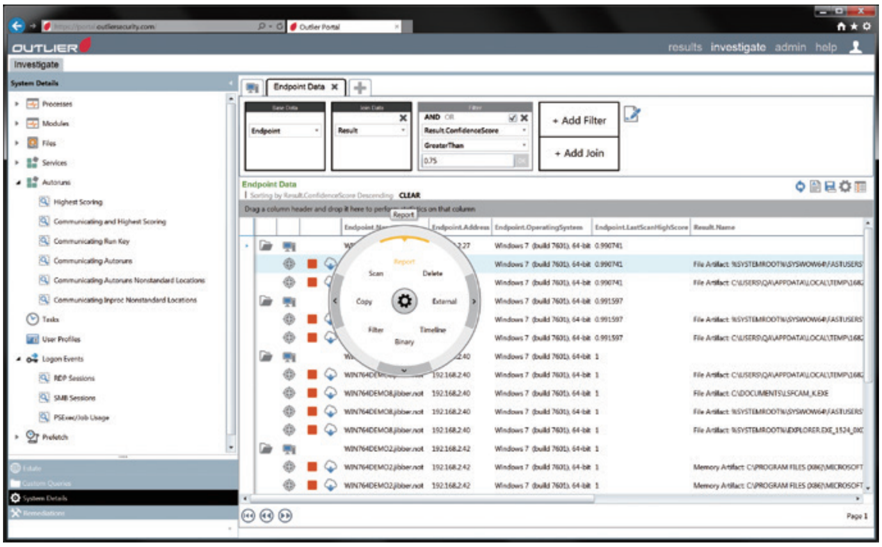
Figure 6-6. Phased Approach to Evidence Collection

An efficient evidence collection process will utilize ETL data analytics techniques to allow for scalable evidence processing. By collecting and correlating data within a database, coincidental artifacts and indicators can be identified quickly, as opposed to always "going back to the source" to identify additional systems of interest. Throughout this process, as IOCs are found and confirmed the data repository can be queried at scale to look for other hosts in the environment that have exhibited the same behavior. This leads to a feedback or "OODA" loop[191] whereby IOCs and scanning rules can be continuously added and updated to produce a thorough understanding of the scope of an incident.

Any systems that a sweep flags for review can then be interrogated in more detail by collecting key forensic artifacts such as those described in Chapter 5, including log files, host and services configuration settings and change histories, file system(s) lists, volatile system data, and user activities

[191] Observe, Orient, Decide, and Act – as opposed to Plan, Do, Check, Act (PDCA)

details. Figure 6-7 below shows an example of sweep aggregated data that is ready for further investigation and collection.

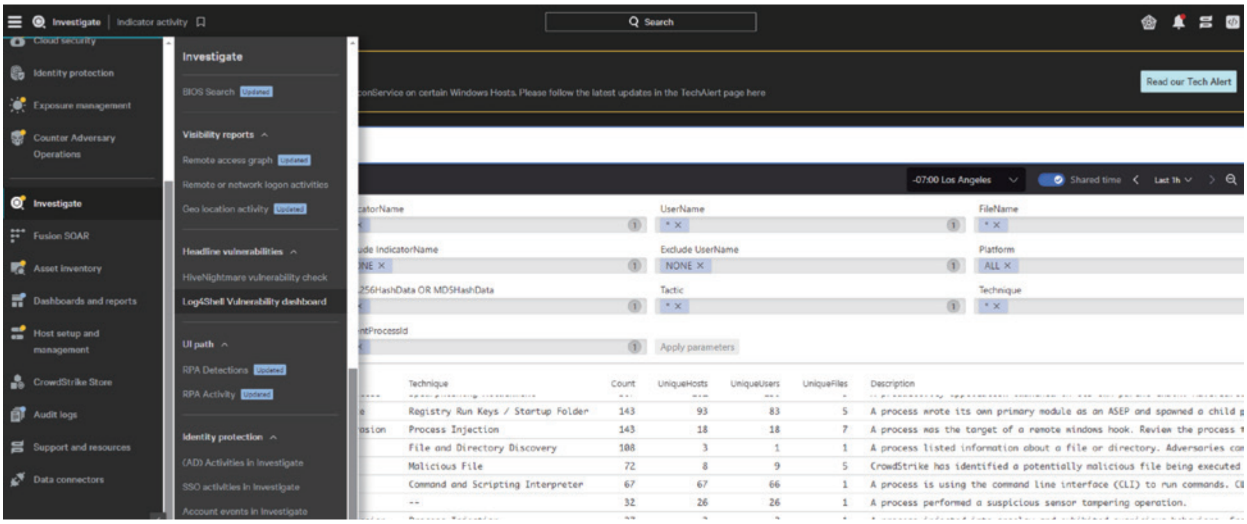


Base Data: Endpoint
Join Data: Result
Filter: AND OR — Result.ConfidenceScore — GreaterThan — 0.75

Endpoint Data
Sorting by Result.ConfidenceScore Descending CLEAR
Drag a column header and drop it here to perform statistics on that column

Endpoint.Name	Endpoint.Address	Endpoint.OperatingSystem	Endpoint.LastScanHighScore	Result.Name
WI	2.27	Windows 7 (build 7601), 64-bit	0.990741	
		Windows 7 (build 7601), 64-bit	0.990741	File Artifact: %SYSTEMROOT%\SYSWOW64\FASTUSERS
		Windows 7 (build 7601), 64-bit	0.990741	File Artifact: C:\USERS\QA\APPDATA\LOCAL\TEMP\168
		Windows 7 (build 7601), 64-bit	0.991597	
		Windows 7 (build 7601), 64-bit	0.991597	File Artifact: %SYSTEMROOT%\SYSWOW64\FASTUSERS
		Windows 7 (build 7601), 64-bit	0.991597	File Artifact: C:\USERS\QA\APPDATA\LOCAL\TEMP\168
Wi	2.40	Windows 7 (build 7601), 64-bit	1	
WIN764DEM	192.168.2.40	Windows 7 (build 7601), 64-bit	1	File Artifact: C:\USERS\QA\APPDATA\LOCAL\TEMP\168
WIN764DEMO8.jibber.not	192.168.2.40	Windows 7 (build 7601), 64-bit	1	File Artifact: C:\DOCUMENTS\LSFCAM_K.EXE
WIN764DEMO8.jibber.not	192.168.2.40	Windows 7 (build 7601), 64-bit	1	File Artifact: %SYSTEMROOT%\SYSWOW64\FASTUSERS
WIN764DEMO8.jibber.not	192.168.2.40	Windows 7 (build 7601), 64-bit	1	File Artifact: %SYSTEMROOT%\EXPLORER.EXE_1524_0X
WIN764DEMO2.jibber.not	192.168.2.42	Windows 7 (build 7601), 64-bit	1	
WIN764DEMO2.jibber.not	192.168.2.42	Windows 7 (build 7601), 64-bit	1	Memory Artifact: C:\PROGRAM FILES (X86)\MICROSOFT
WIN764DEMO2.jibber.not	192.168.2.42	Windows 7 (build 7601), 64-bit	1	Memory Artifact: C:\PROGRAM FILES (X86)\MICROSOFT

Figure 6-7a. Outlier Security Sweep Collection and Aggregation of Evidence



onService on certain Windows Hosts. Please follow the latest updates in the TechAlert page here

catorName | UserName: * | FileName: *
ude IndicatorName: NONE | Exclude UserName: NONE | Platform: ALL
256HashData OR MD5HashData | Tactic: * | Technique: *
ntProcessId

Technique	Count	UniqueHosts	UniqueUsers	UniqueFiles	Description
Registry Run Keys / Startup Folder	143	93	83	5	A process wrote its own primary module as an ASEP and spawned a child p
Process Injection	143	18	18	7	A process was the target of a remote windows hook. Review the process t
File and Directory Discovery	108	3	1	1	A process listed information about a file or directory. Adversaries can
Malicious File	72	8	9	5	CrowdStrike has identified a potentially malicious file being executed
Command and Scripting Interpreter	67	67	66	1	A process is using the command line interface (CLI) to run commands. CL
--	32	26	26	1	A process performed a suspicious sensor tampering operation.

Figure 6-7b. Crowdstrike Falcon Collection and Aggregation of Evidence

Manual Evidence Collection

Once systems of interest have been identified using the sweep discovery approach, specific information about configuration and use history may be necessary to discover evidence of the crime. Although automated enterprise tools and software applications can assist with the collection and analysis of evidence, there may not be enough details from systemic alerts or sweep evidence to form conclusions or satisfy legal and/or regulatory requirements. Once systems of interest have been identified, certain artifacts should be collected. An essential determination must first be made about the organizational or investigation policy concerning the collection of evidence.

Digital forensics analysts spend approximately 95% of their time on less than 1% (by volume) of artifacts that are available for collection from computers. In general, available artifacts include:

1. Volatile system information such as network connections and active processes (and their resources)
2. Volatile active and physical memory pages
3. File system contents (including files, programs, and history/logs)
4. Hardware configurations (including disk volumes and attached devices)
5. Software configurations (including operating system, enterprise management, and user applications)

The noted artifacts can be collected using either a metadata or a content-oriented acquisition method. The appropriate method depends upon the guiding collection policy or instructions that the investigator must follow.

Metadata-oriented acquisition (i.e. Investigate, the second phase) applies to the 1% of artifacts that analysts spend 95% of their time on. It focuses on the acquisition of metadata about files, log contents, and volatile system information from native tools. Contents of files (other than specified logs) are not collected, as the primary interest of an analyst when assessing such metadata is to determine a timeline of events and relative evidence that describes cybercrime activities. Metadata-oriented acquisition for Microsoft Windows computers, for example, typically includes the following files:

- $MFT and $USNJrnl
- REG hives (System, Software, Security, and SAM)
- User history (NTUser.DAT, USRClass.DAT, and Internet – i.e. Index.DAT, etc.)
- EVT/EVTX logs (Application, Security, and System)
- Antivirus logs
- Volatile system data (TASKLIST, NETSTAT, ARP, IPCONFIG, and Autorun Entries)

Similar information can be collected from Mac OSX, Linux, and other operating systems for metadata-oriented acquisition. The primary reason for such a lightweight acquisition is to quickly and efficiently collect sufficient evidence that is useful to the investigation. As with the sweep discovery collection, this collection can be assisted with enterprise tools and ETL with database analytics can efficiently reveal coincidence and details in evidence that is unavailable to independent system analysts.

Sometimes, either a policy or technical need will dictate a more complete content-oriented acquisition to support the collection of evidence. This “third phase” (i.e. Collect) may be necessary because lawyers or organizational risk management policies, often based upon regulatory mandates, require full disk imaging (bit for bit forensic copying of a physical hard drive and sometimes active memory contents). In other circumstances, it may be necessary to collect a “memory image” to perform additional technical or content analysis. In these cases, there is little choice but to either utilize an enterprise forensic toolset that can connect with remote hosts or to physically collect image(s) from the computer. Content-oriented acquisitions are the most expensive in terms of resource allocations because specific (and limited) skills, tools, time, and associated costs are required. Sweep discovery and metadata-oriented acquisitions of evidence can employ ETL and data analytics at the scale of the collected enterprise information; content-oriented acquisition is typically a one-to-one relationship of acquired images and analysis.

Because of the varied costs and efficiencies in these phases for determining the scope and impact of cybercrimes, organizations should review jurisdictional requirements- including regulatory and legal mandates of evidence production- according to types of cybercrimes they may experience (see Chapter 2). Those requirements should be reviewed against the skills, knowledge, experience, and tools available. The combination of requirements and resources should then form guiding policies and procedures for intelligent and efficient evidence collection.

Best practices in industry and law enforcement include:

1. The use of systemic collection to alert potential cybercrimes from patterns/IOCs of anomalous activities.
2. Periodic sweeps of enterprise computers and related endpoints to discover systems of interest or anomalous user behavior
3. Manual acquisitions of metadata-oriented artifacts to examine for evidence
4. Only when required by policy, acquiring content-oriented artifacts for the retention and/or examination of cybercrime evidence

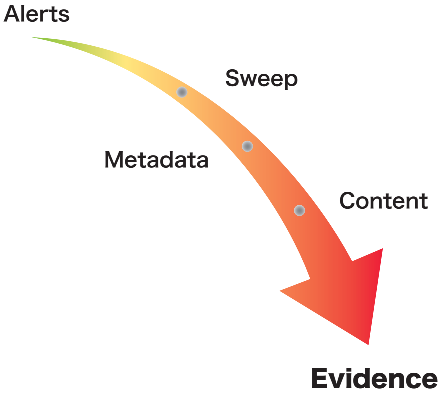
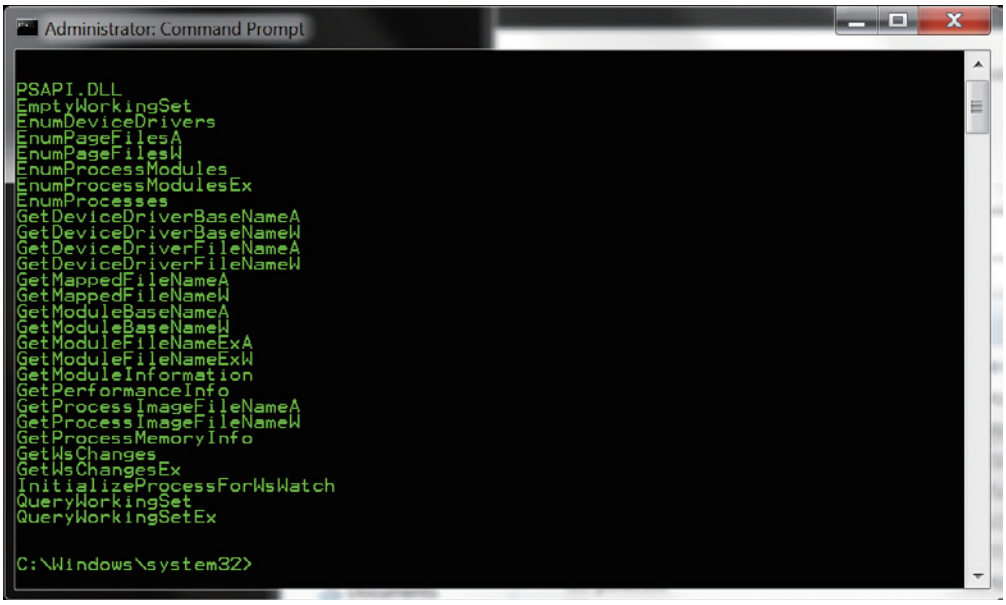


Figure 6-8. Methods of Evidence Collection

Native Tools

A "manual collection" approach uses native and third-party tools to collect evidence. Native tools include utilities within an operating system that enable administrators or users (depending upon their permissions settings) to query information about the computer' s services, configuration, and history of use. Third-party tools can provide similar information, but perform correlations of independent artifacts of data from the computer for designed objectives. Native and third-party tools make use of "Application Programming Interface" (API) function calls to underlying operating and file system details using scripted instructions, often as compiled programs. Not coincidentally, malware also uses API function calls to achieve similar functional objectives including remote access, programming, information access, and control of the computer.

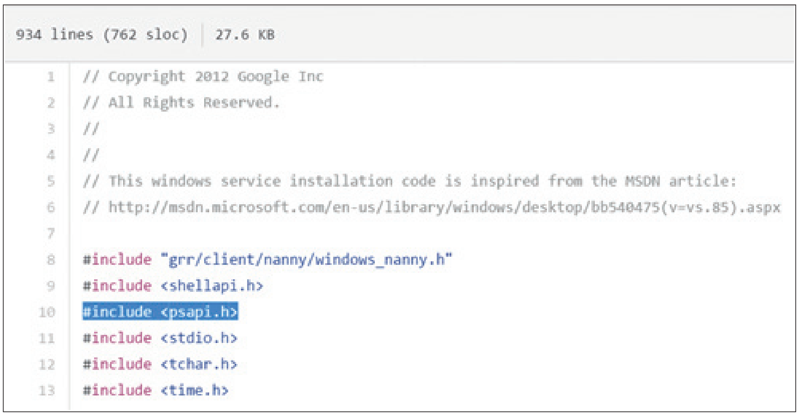
As an example, two primary APIs are common and often used by operating system information collection tools: PSAPI and NETAPI. The Process Status (PS) API includes the native functions available to programs and query information about processes. For example, Figure 6-9 below shows the function calls made by the "TASKLIST.EXE" command via resource calls on the "PSAPI.DLL" that contains the API instruction sets[192]:



```
PSAPI.DLL
EmptyWorkingSet
EnumDeviceDrivers
EnumPageFilesA
EnumPageFilesW
EnumProcessModules
EnumProcessModulesEx
EnumProcesses
GetDeviceDriverBaseNameA
GetDeviceDriverBaseNameW
GetDeviceDriverFileNameA
GetDeviceDriverFileNameW
GetMappedFileNameA
GetMappedFileNameW
GetModuleBaseNameA
GetModuleBaseNameW
GetModuleFileNameExA
GetModuleFileNameExW
GetModuleInformation
GetPerformanceInfo
GetProcessImageFileNameA
GetProcessImageFileNameW
GetProcessMemoryInfo
GetWsChanges
GetWsChangesEx
InitializeProcessForWsWatch
QueryWorkingSet
QueryWorkingSetEx

C:\Windows\system32>
```

Figure 6-9. TASKLIST use of PSAPI

The Network (NET) APIs provide similar functional calls for network statistics (NETSTAT.EXE)[193], network management (NETSH.EXE)[194], and use details (NET.EXE). The described utilities are functionally similar in all operating systems and provide fundamental evidence collection capabilities with native as well as third-party tools. For example, the Google Rapid Response[195] incident response toolkit source code displayed in Figure 6-10 below details the "included" resource libraries that the program relies upon:



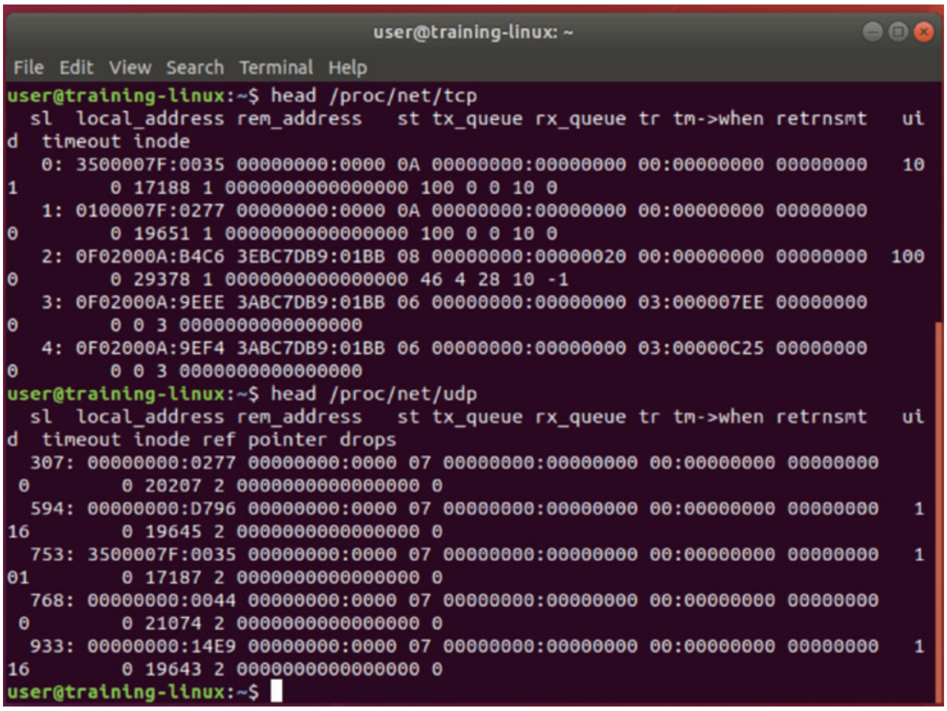
```
// Copyright 2012 Google Inc
// All Rights Reserved.
//
//
// This windows service installation code is inspired from the MSDN article:
// http://msdn.microsoft.com/en-us/library/windows/desktop/bb540475(v=vs.85).aspx

#include "grr/client/nanny/windows_nanny.h"
#include <shellapi.h>
#include <psapi.h>
#include <stdio.h>
#include <tchar.h>
#include <time.h>
```

Figure 6-10. Third-party use of PSAPI

Even without common utilities such as NETSTAT, an experienced system analyst will always be

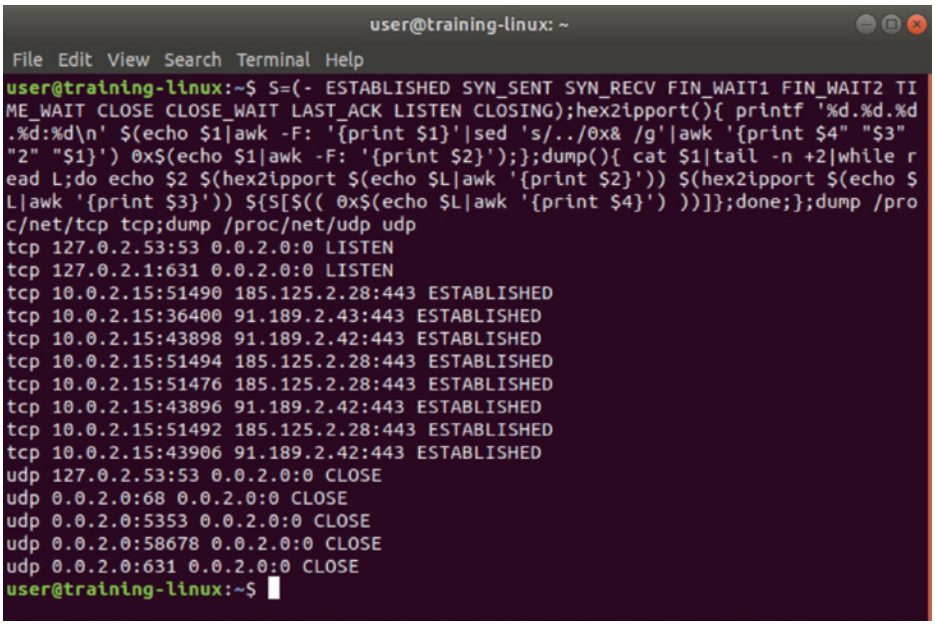
[192] https://msdn.microsoft.com/en-us/library/windows/desktop/ms684884(v=vs.85).aspx
[193] https://msdn.microsoft.com/en-us/library/windows/desktop/bb525390(v=vs.85).aspx
[194] https://msdn.microsoft.com/en-us/library/windows/desktop/aa370675(v=vs.85).aspx
[195] https://github.com/google/grr

able to collect useful information from a system of interest[196] with simple methods, as demonstrated in Figure 6-11a and 6-11b below. It is important to note, however, that 32 and 64-bit process information- particularly resources (DLL' s and Shared Objects)- are not equally accessible with native (and many third-party) tools. Any analysis of collected evidence should take this into account.



```
user@training-linux:~$ head /proc/net/tcp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   ui
d  timeout inode
   0: 3500007F:0035 00000000:0000 0A 00000000:00000000 00:00000000 00000000   10
1         0 17188 1 0000000000000000 100 0 0 10 0
   1: 0100007F:0277 00000000:0000 0A 00000000:00000000 00:00000000 00000000
0         0 19651 1 0000000000000000 100 0 0 10 0
   2: 0F02000A:B4C6 3EBC7DB9:01BB 08 00000000:00000020 00:00000000 00000000  100
0         0 29378 1 0000000000000000 46 4 28 10 -1
   3: 0F02000A:9EEE 3ABC7DB9:01BB 06 00000000:00000000 03:000007EE 00000000
0         0 0 3 0000000000000000
   4: 0F02000A:9EF4 3ABC7DB9:01BB 06 00000000:00000000 03:00000C25 00000000
0         0 0 3 0000000000000000
user@training-linux:~$ head /proc/net/udp
  sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   ui
d  timeout inode ref pointer drops
  307: 00000000:0277 00000000:0000 07 00000000:00000000 00:00000000 00000000
 0         0 20207 2 0000000000000000 0
  594: 00000000:D796 00000000:0000 07 00000000:00000000 00:00000000 00000000   1
16         0 19645 2 0000000000000000 0
  753: 3500007F:0035 00000000:0000 07 00000000:00000000 00:00000000 00000000   1
01         0 17187 2 0000000000000000 0
  768: 00000000:0044 00000000:0000 07 00000000:00000000 00:00000000 00000000
 0         0 21074 2 0000000000000000 0
  933: 00000000:14E9 00000000:0000 07 00000000:00000000 00:00000000 00000000   1
16         0 19643 2 0000000000000000 0
user@training-linux:~$ 
```

Figure 6-11a. Native NET statistics from Linux (raw)



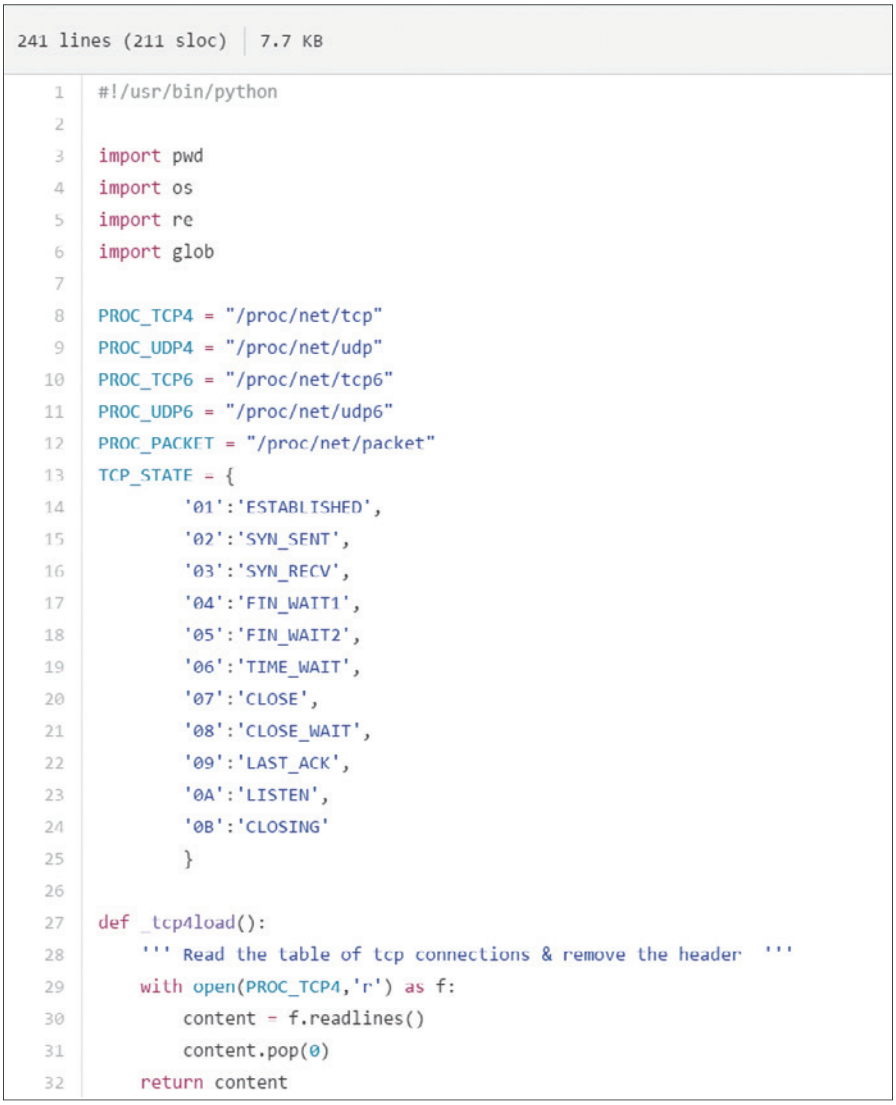
```
user@training-linux:~$ S=(- ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2 TI
ME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING);hex2ipport(){ printf '%d.%d.%d
.%d:%d\n' $(echo $1|awk -F: '{print $1}'|sed 's/../0x& /g'|awk '{print $4" "$3"
"2" "$1}') 0x$(echo $1|awk -F: '{print $2}');};dump(){ cat $1|tail -n +2|while r
ead L;do echo $2 $(hex2ipport $(echo $L|awk '{print $2}')) $(hex2ipport $(echo $
L|awk '{print $3}')) ${S[$(( 0x$(echo $L|awk '{print $4}') ))]};done;};dump /pro
c/net/tcp tcp;dump /proc/net/udp udp
tcp 127.0.2.53:53 0.0.2.0:0 LISTEN
tcp 127.0.2.1:631 0.0.2.0:0 LISTEN
tcp 10.0.2.15:51490 185.125.2.28:443 ESTABLISHED
tcp 10.0.2.15:36400 91.189.2.43:443 ESTABLISHED
tcp 10.0.2.15:43898 91.189.2.42:443 ESTABLISHED
tcp 10.0.2.15:51494 185.125.2.28:443 ESTABLISHED
tcp 10.0.2.15:51476 185.125.2.28:443 ESTABLISHED
tcp 10.0.2.15:43896 91.189.2.42:443 ESTABLISHED
tcp 10.0.2.15:51492 185.125.2.28:443 ESTABLISHED
tcp 10.0.2.15:43906 91.189.2.42:443 ESTABLISHED
udp 127.0.2.53:53 0.0.2.0:0 CLOSE
udp 0.0.2.0:68 0.0.2.0:0 CLOSE
udp 0.0.2.0:5353 0.0.2.0:0 CLOSE
udp 0.0.2.0:58678 0.0.2.0:0 CLOSE
udp 0.0.2.0:631 0.0.2.0:0 CLOSE
user@training-linux:~$ 
```

Figure 6-11b. Native NET statistics from Linux (translated)

As noted, NETAPI information can also be called with third-party tools. In Figure 6-12 below, a

[196] Note that the addresses are displayed as reverse HEXIDECIMAL format (0100007F = 127.0.0.1)

python script for Linux is used to return network connection statistics from a PS call[197]:

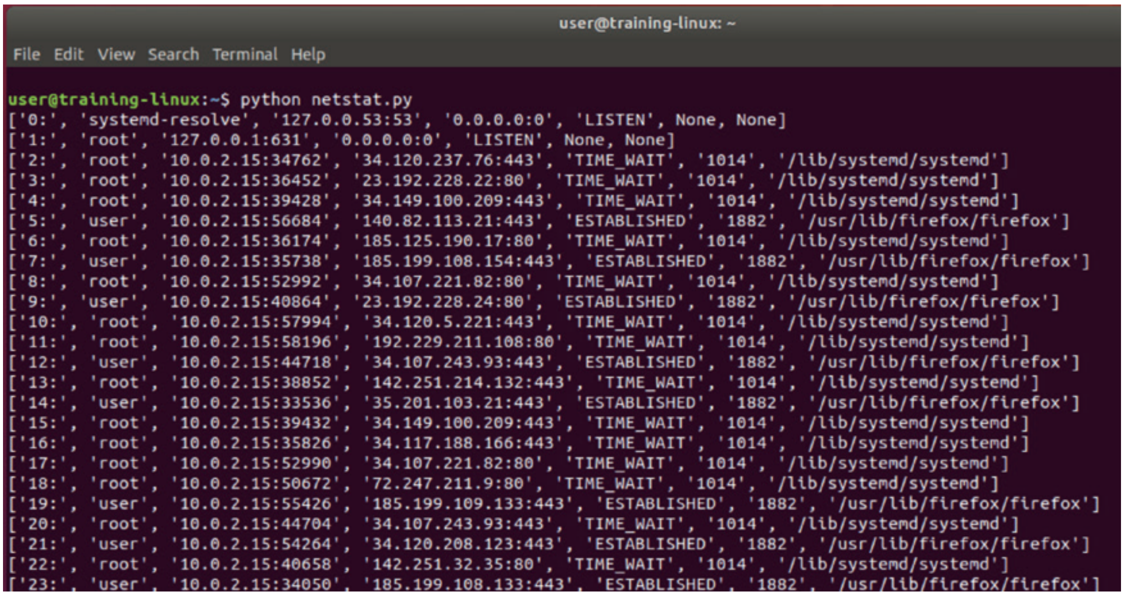


241 lines (211 sloc) | 7.7 KB

```
#!/usr/bin/python

import pwd
import os
import re
import glob

PROC_TCP4 = "/proc/net/tcp"
PROC_UDP4 = "/proc/net/udp"
PROC_TCP6 = "/proc/net/tcp6"
PROC_UDP6 = "/proc/net/udp6"
PROC_PACKET = "/proc/net/packet"
TCP_STATE = {
        '01':'ESTABLISHED',
        '02':'SYN_SENT',
        '03':'SYN_RECV',
        '04':'FIN_WAIT1',
        '05':'FIN_WAIT2',
        '06':'TIME_WAIT',
        '07':'CLOSE',
        '08':'CLOSE_WAIT',
        '09':'LAST_ACK',
        '0A':'LISTEN',
        '0B':'CLOSING'
        }

def _tcp4load():
    ''' Read the table of tcp connections & remove the header  '''
    with open(PROC_TCP4,'r') as f:
        content = f.readlines()
        content.pop(0)
    return content
```

Figure 6-12a. Third-party use of PS for NETSTAT (netstat.py)

[197] https://github.com/da667/netstat/blob/master/netstat.py



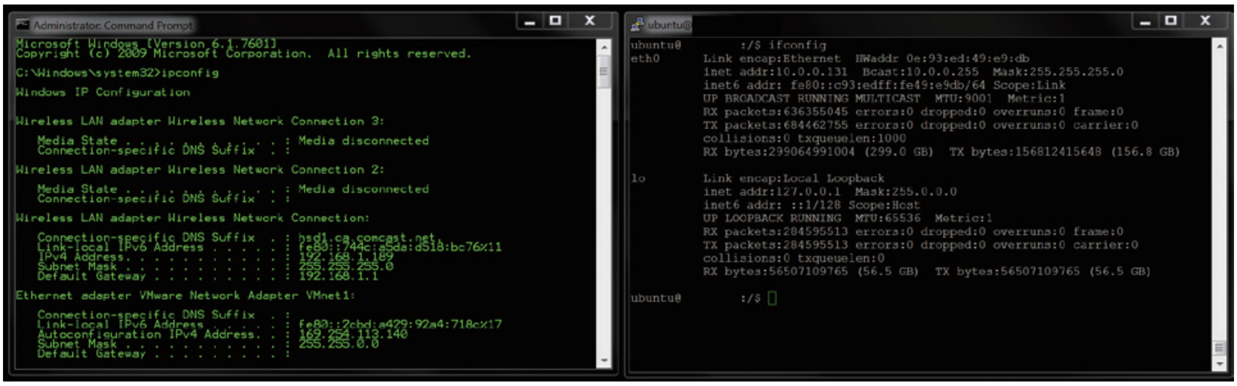
```
user@training-linux:~$ python netstat.py
['0:', 'systemd-resolve', '127.0.0.53:53', '0.0.0.0:0', 'LISTEN', None, None]
['1:', 'root', '127.0.0.1:631', '0.0.0.0:0', 'LISTEN', None, None]
['2:', 'root', '10.0.2.15:34762', '34.120.237.76:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['3:', 'root', '10.0.2.15:36452', '23.192.228.22:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['4:', 'root', '10.0.2.15:39428', '34.149.100.209:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['5:', 'user', '10.0.2.15:56684', '140.82.113.21:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['6:', 'root', '10.0.2.15:36174', '185.125.190.17:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['7:', 'user', '10.0.2.15:35738', '185.199.108.154:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['8:', 'root', '10.0.2.15:52992', '34.107.221.82:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['9:', 'user', '10.0.2.15:40864', '23.192.228.24:80', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['10:', 'root', '10.0.2.15:57994', '34.120.5.221:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['11:', 'root', '10.0.2.15:58196', '192.229.211.108:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['12:', 'user', '10.0.2.15:44718', '34.107.243.93:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['13:', 'root', '10.0.2.15:38852', '142.251.214.132:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['14:', 'user', '10.0.2.15:33536', '35.201.103.21:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['15:', 'root', '10.0.2.15:39432', '34.149.100.209:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['16:', 'root', '10.0.2.15:35826', '34.117.188.166:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['17:', 'root', '10.0.2.15:52990', '34.107.221.82:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['18:', 'root', '10.0.2.15:50672', '72.247.211.9:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['19:', 'user', '10.0.2.15:55426', '185.199.109.133:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['20:', 'root', '10.0.2.15:44704', '34.107.243.93:443', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['21:', 'user', '10.0.2.15:54264', '34.120.208.123:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
['22:', 'root', '10.0.2.15:40658', '142.251.32.35:80', 'TIME_WAIT', '1014', '/lib/systemd/systemd']
['23:', 'user', '10.0.2.15:34050', '185.199.108.133:443', 'ESTABLISHED', '1882', '/usr/lib/firefox/firefox']
```

Figure 6-12b. Third-party use of PS for NETSTAT (netstat.py)

There are many ways to access and collect evidence from hosts with native or third-party tools. Organizations must make practical decisions when planning for cyber investigative functions or when hiring outside support. There is often a tradeoff between skills and tools: no expensive tools will replace inexpensive and inexperienced staff, yet expensive and experienced staff may not require expensive tools. Fortunately, there are many native and third-party tools to assist inexperienced staff if they understand what and why to collect such information.

●Network

Both Windows and Linux systems[198] contain utilities to query the status of network configurations and connections. These include hardware network address information (IPCONFIG and ifconfig) as well as services and status (netstat), as shown in Figure 6-13 below:



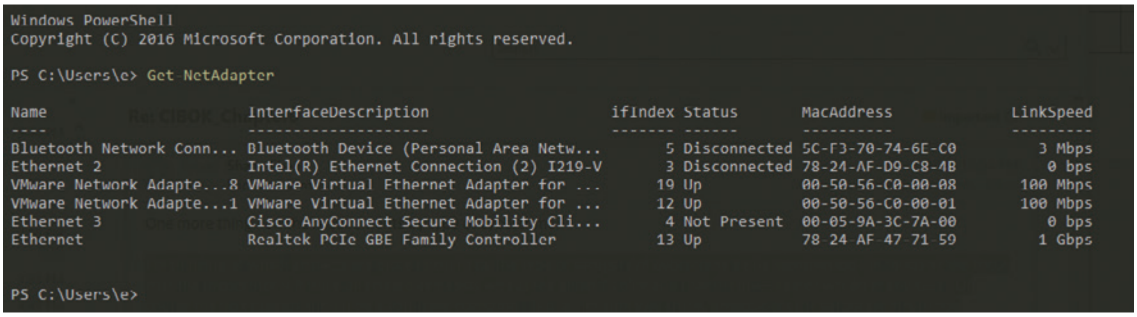
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : hsd1.ca.comcast.net
   Link-local IPv6 Address . . . . . : fe80::744c:a5da:d518:bc76%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.189
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2cbd:a429:92a4:718c%17
   Autoconfiguration IPv4 Address. . : 169.254.113.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

```
ubuntu@        :/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0e:93:ed:49:e9:db
          inet addr:10.0.0.131  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::c93:edff:fe49:e9db/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:636355045 errors:0 dropped:0 overruns:0 frame:0
          TX packets:684462755 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:299064991004 (299.0 GB)  TX bytes:156812415648 (156.8 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:284595513 errors:0 dropped:0 overruns:0 frame:0
          TX packets:284595513 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56507109765 (56.5 GB)  TX bytes:56507109765 (56.5 GB)

ubuntu@        :/$ 
```

Figure 6-13. Windows IPCONFIG and Linux ifconfig

[198] Linux is used for demonstration purposes throughout this chapter, as it has similarities to several Unix operating systems and to OSX (Apple) as well as various mobile, networking, and even operating systems that serve DCS equipment (DCU/RTU, etc.).

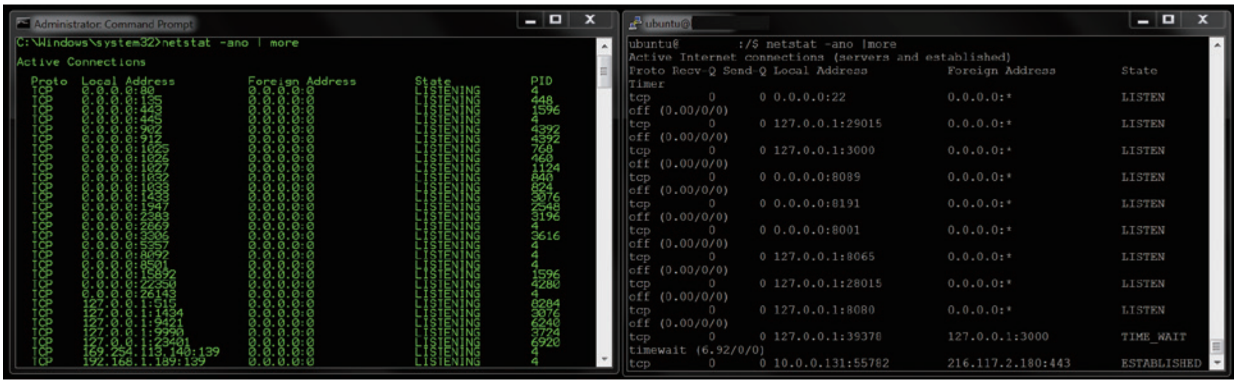
Tools such as PowerShell (which has recently been extended for Linux support as well[199]) are very capable of collecting a wide range of artifacts for evidence. Although PowerShell is not a scripting or programming language, it does support automated administration tasks including information collection. Data returned from PowerShell scripts can be aggregated in a central location and analyzed for anomalies. Data that can be collected by PowerShell includes operating system details, installed programs, running processes, network information, open files, network shares, firewall configuration, and more. PowerShell can be extended using any Microsoft .net framework language like C#, which allows for more complex PowerShell functionality to be created. PowerShell management utilities are updated with each patch issued by Microsoft, so some functions (such as Get-NetAdapter, shown in Figure 6-15, which is packaged with Windows 8.1/2012) may require script creation[200].



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\e> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                    ------- ------       ----------             ---------
Bluetooth Network Conn... Bluetooth Device (Personal Area Netw...       5 Disconnected 5C-F3-70-74-6E-C0         3 Mbps
Ethernet 2                Intel(R) Ethernet Connection (2) I219-V       3 Disconnected 78-24-AF-D9-C8-4B         0 bps
VMware Network Adapte...8 VMware Virtual Ethernet Adapter for ...      19 Up           00-50-56-C0-00-08       100 Mbps
VMware Network Adapte...1 VMware Virtual Ethernet Adapter for ...      12 Up           00-50-56-C0-00-01       100 Mbps
Ethernet 3                Cisco AnyConnect Secure Mobility Cli...       4 Not Present  00-05-9A-3C-7A-00         0 bps
Ethernet                  Realtek PCIe GBE Family Controller           13 Up           78-24-AF-47-71-59         1 Gbps

PS C:\Users\e>
```

Figure 6-14. Windows POWERSHELL Get-NetAdapter

Network statistics about active processes are very useful for determining associated services configurations. A simple technique that investigators can utilize is to associate NETSTAT with PS (TASKLIST or LSOF) output by the process identifier (PID), as shown in Figures 6-15 and 6-16 below. Malware is known to hook legitimate service processes, such as svchost.exe or dllhost32.exe or etc., so it is also useful to include open files in related outputs.



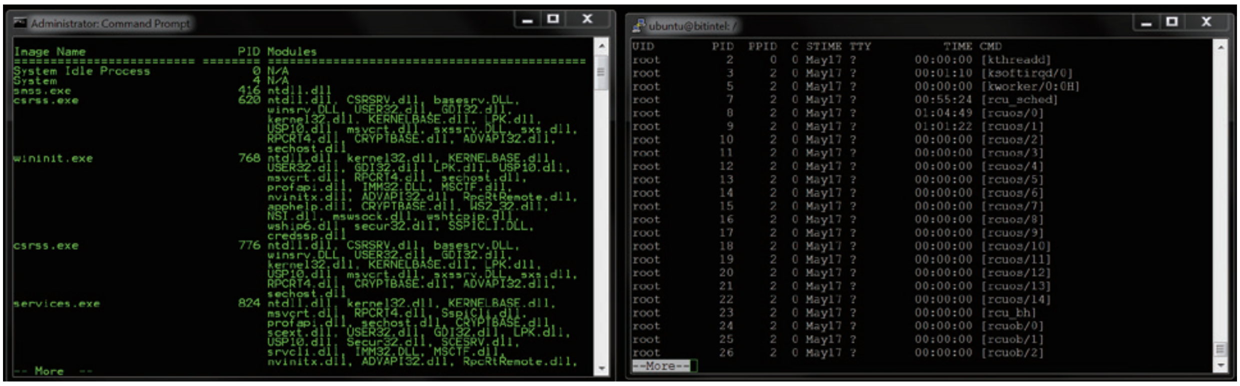
```
C:\Windows\system32>netstat -ano | more

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       448
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       1596
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4392
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4392
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       768
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       460
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       1124
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING       840
  TCP    0.0.0.0:1033           0.0.0.0:0              LISTENING       824
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       3076
  TCP    0.0.0.0:1947           0.0.0.0:0              LISTENING       2548
  TCP    0.0.0.0:2383           0.0.0.0:0              LISTENING       3196
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       3616
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:8092           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:8501           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:15892          0.0.0.0:0              LISTENING       1596
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING       4280
  TCP    0.0.0.0:26143          0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:515          0.0.0.0:0              LISTENING       8284
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       3076
  TCP    127.0.0.1:9421         0.0.0.0:0              LISTENING       6240
  TCP    127.0.0.1:9990         0.0.0.0:0              LISTENING       3724
  TCP    127.0.0.1:23401        0.0.0.0:0              LISTENING       6920
  TCP    169.254.113.140:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.1.189:139      0.0.0.0:0              LISTENING       4
```

```
ubuntu@[redacted]:/$ netstat -ano |more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Timer
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:29015         0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 0.0.0.0:8191            0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 0.0.0.0:8001            0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:8065          0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:28015         0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
off (0.00/0/0)
tcp        0      0 127.0.0.1:39378         127.0.0.1:3000          TIME_WAIT
timewait (6.92/0/0)
tcp        0      0 10.0.0.131:55782        216.117.2.180:443       ESTABLISHED
```

Figure 6-15. Windows and Linux netstat -ano

[199] https://blogs.msdn.microsoft.com/powershell/2015/05/05/powershell-dsc-for-linux-is-now-available/

[200] https://blogs.technet.microsoft.com/heyscriptingguy/2014/01/15/using-powershell-to-find-connected-network-adapters/

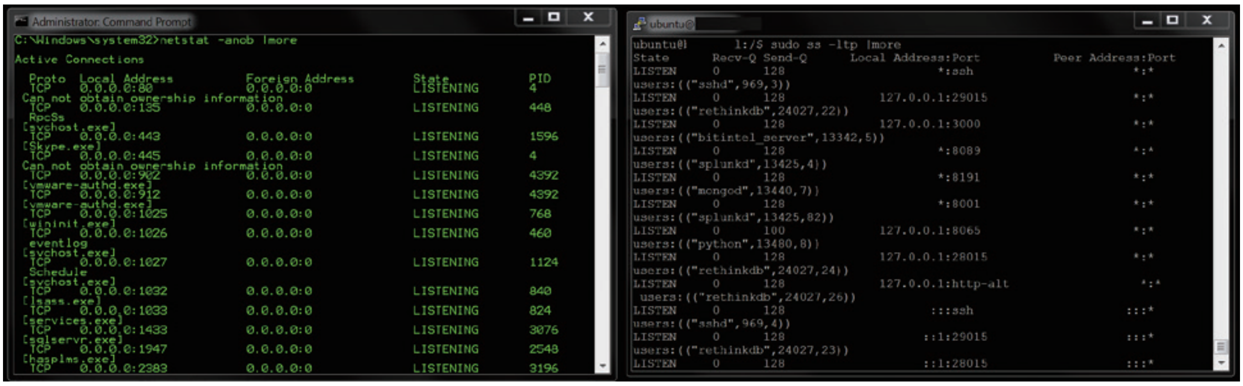


```
Image Name                     PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       416 ntdll.dll
csrss.exe                      620 ntdll.dll, CSRSRV.dll, basesrv.DLL,
                                   winsrv.DLL, USER32.dll, GDI32.dll,
                                   kernel32.dll, KERNELBASE.dll, LPK.dll,
                                   USP10.dll, msvcrt.dll, sxssrv.DLL, sxs.dll,
                                   RPCRT4.dll, CRYPTBASE.dll, ADVAPI32.dll,
                                   sechost.dll
wininit.exe                    768 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
                                   msvcrt.dll, RPCRT4.dll, sechost.dll,
                                   profapi.dll, IMM32.DLL, MSCTF.dll,
                                   nvinitx.dll, ADVAPI32.dll, RpcRtRemote.dll,
                                   apphelp.dll, CRYPTBASE.dll, WS2_32.dll,
                                   NSI.dll, mswsock.dll, wshtcpip.dll,
                                   wship6.dll, secur32.dll, SSPICLI.DLL,
                                   credssp.dll
csrss.exe                      776 ntdll.dll, CSRSRV.dll, basesrv.DLL,
                                   winsrv.DLL, USER32.dll, GDI32.dll,
                                   kernel32.dll, KERNELBASE.dll, LPK.dll,
                                   USP10.dll, msvcrt.dll, sxssrv.DLL, sxs.dll,
                                   RPCRT4.dll, CRYPTBASE.dll, ADVAPI32.dll,
                                   sechost.dll
services.exe                   824 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   msvcrt.dll, RPCRT4.dll, SspiCli.dll,
                                   profapi.dll, sechost.dll, CRYPTBASE.dll,
                                   scext.dll, USER32.dll, GDI32.dll, LPK.dll,
                                   USP10.dll, Secur32.dll, SCESRV.dll,
                                   srvcli.dll, IMM32.DLL, MSCTF.dll,
                                   nvinitx.dll, ADVAPI32.dll, RpcRtRemote.dll,
-- More --
```

```
UID        PID  PPID  C STIME TTY          TIME CMD
root         2     0  0 May17 ?        00:00:00 [kthreadd]
root         3     2  0 May17 ?        00:01:10 [ksoftirqd/0]
root         5     2  0 May17 ?        00:00:00 [kworker/0:0H]
root         7     2  0 May17 ?        00:55:24 [rcu_sched]
root         8     2  0 May17 ?        01:04:49 [rcuos/0]
root         9     2  0 May17 ?        01:01:22 [rcuos/1]
root        10     2  0 May17 ?        00:00:00 [rcuos/2]
root        11     2  0 May17 ?        00:00:00 [rcuos/3]
root        12     2  0 May17 ?        00:00:00 [rcuos/4]
root        13     2  0 May17 ?        00:00:00 [rcuos/5]
root        14     2  0 May17 ?        00:00:00 [rcuos/6]
root        15     2  0 May17 ?        00:00:00 [rcuos/7]
root        16     2  0 May17 ?        00:00:00 [rcuos/8]
root        17     2  0 May17 ?        00:00:00 [rcuos/9]
root        18     2  0 May17 ?        00:00:00 [rcuos/10]
root        19     2  0 May17 ?        00:00:00 [rcuos/11]
root        20     2  0 May17 ?        00:00:00 [rcuos/12]
root        21     2  0 May17 ?        00:00:00 [rcuos/13]
root        22     2  0 May17 ?        00:00:00 [rcuos/14]
root        23     2  0 May17 ?        00:00:00 [rcu_bh]
root        24     2  0 May17 ?        00:00:00 [rcuob/0]
root        25     2  0 May17 ?        00:00:00 [rcuob/1]
root        26     2  0 May17 ?        00:00:00 [rcuob/2]
--More--
```

Figure 6-16. Windows TASKLIST /M and Linux ps -df

Another (simpler) method is to show the process identity by its network connection information, as shown in Figure 6-17 below:

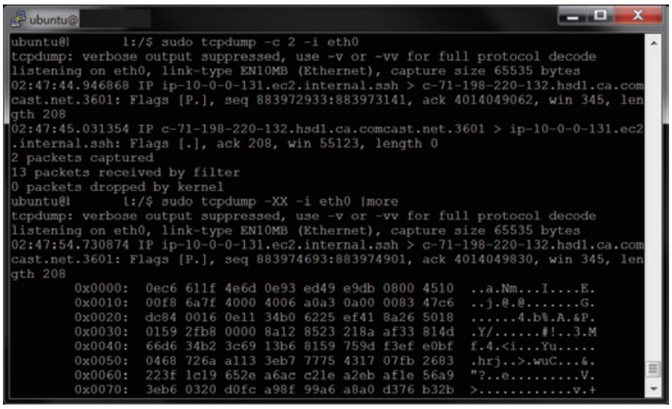


```
C:\Windows\system32>netstat -anob |more

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       448
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       1596
 [Skype.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4392
 [vmware-authd.exe]
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4392
 [vmware-authd.exe]
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       768
 [wininit.exe]
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING       460
  eventlog
 [svchost.exe]
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       1124
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING       840
 [lsass.exe]
  TCP    0.0.0.0:1033           0.0.0.0:0              LISTENING       824
 [services.exe]
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       3076
 [sqlservr.exe]
  TCP    0.0.0.0:1947           0.0.0.0:0              LISTENING       2548
 [hasplms.exe]
  TCP    0.0.0.0:2383           0.0.0.0:0              LISTENING       3196
```

```
ubuntu@l      l:/$ sudo ss -ltp |more
State      Recv-Q Send-Q      Local Address:Port          Peer Address:Port
LISTEN     0      128                     *:ssh                      *:*
users:(("sshd",969,3))
LISTEN     0      128             127.0.0.1:29015                    *:*
users:(("rethinkdb",24027,22))
LISTEN     0      128             127.0.0.1:3000                     *:*
users:(("bitintel_server",13342,5))
LISTEN     0      128                     *:8089                     *:*
users:(("splunkd",13425,4))
LISTEN     0      128                     *:8191                     *:*
users:(("mongod",13440,7))
LISTEN     0      128                     *:8001                     *:*
users:(("splunkd",13425,82))
LISTEN     0      100             127.0.0.1:8065                     *:*
users:(("python",13480,8))
LISTEN     0      128             127.0.0.1:28015                    *:*
users:(("rethinkdb",24027,24))
LISTEN     0      128             127.0.0.1:http-alt                  *:*
 users:(("rethinkdb",24027,26))
LISTEN     0      128                    :::ssh                     :::*
users:(("sshd",969,4))
LISTEN     0      128                  ::1:29015                    :::*
users:(("rethinkdb",24027,23))
LISTEN     0      128                  ::1:28015                    :::*
```

Figure 6-17. Windows NETSTAT -ANOB and Linux ss -ltp

Network packet captures are also very useful artifacts to examine for evidence. Linux systems include a utility called 'tcpdump' which allows network traffic collection on a specified interface, as shown in Figure 6-18 below. This collection can then be analyzed with text editors or other tools such as "Wireshark"[201] to investigate network communications.

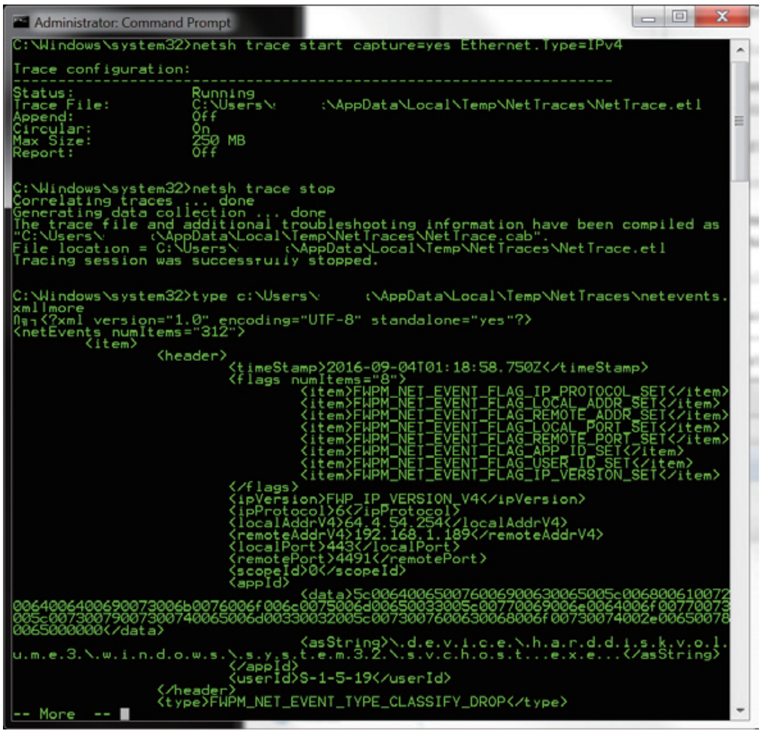


```
ubuntu@l      1:/$ sudo tcpdump -c 2 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
02:47:44.946868 IP ip-10-0-0-131.ec2.internal.ssh > c-71-198-220-132.hsd1.ca.com
cast.net.3601: Flags [P.], seq 883972933:883973141, ack 4014049062, win 345, len
gth 208
02:47:45.031354 IP c-71-198-220-132.hsd1.ca.comcast.net.3601 > ip-10-0-0-131.ec2
.internal.ssh: Flags [.], ack 208, win 55123, length 0
2 packets captured
13 packets received by filter
0 packets dropped by kernel
ubuntu@l      l:/$ sudo tcpdump -XX -i eth0 |more
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
02:47:54.730874 IP ip-10-0-0-131.ec2.internal.ssh > c-71-198-220-132.hsd1.ca.com
cast.net.3601: Flags [P.], seq 883974693:883974901, ack 4014049830, win 345, len
gth 208
        0x0000:  0ec6 611f 4e6d 0e93 ed49 e9db 0800 4510  ..a.Nm...I.....E.
        0x0010:  00f8 6a7f 4000 4006 a0a3 0a00 0083 47c6  ..j.@.@.......G.
        0x0020:  dc84 0016 0e11 34b0 6225 ef41 8a26 5018  ......4.b%.A.&P.
        0x0030:  0159 2fb8 0000 8a12 8523 218a af33 814d  .Y/......#!..3.M
        0x0040:  66d6 34b2 3c69 13b6 8159 759d f3ef e0bf  f.4.<i....Yu.....
        0x0050:  0468 726a a113 3eb7 7775 4317 07fb 2683  .hrj..>.wuC....&.
        0x0060:  223f 1c19 652e a6ac c21e a2eb af1e 56a9  "?..e..........V.
        0x0070:  3eb6 0320 d0fc a98f 99a6 a8a0 d376 b32b  >.............v.+
```

Figure 6-18. Linux tcpdump

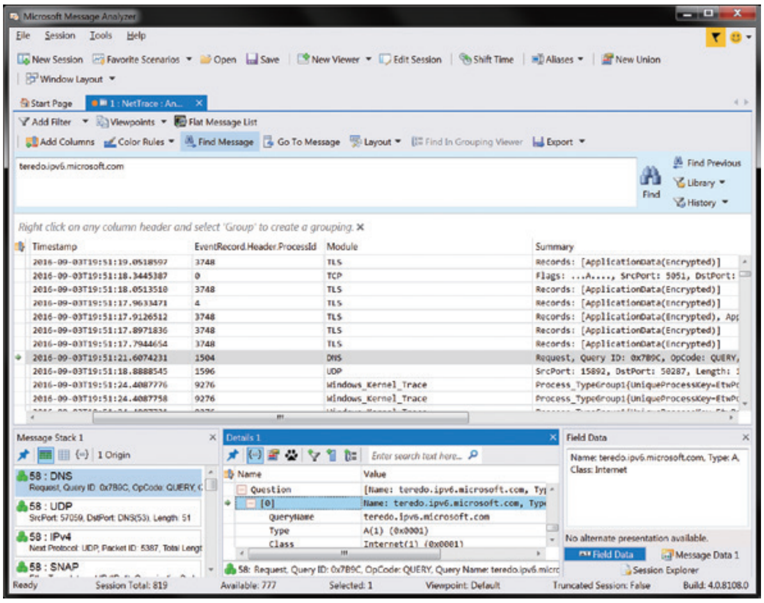
[201] https://www.wireshark.org/

A similar utility exists in Windows 7 (NETSH) that allows the collection of network information about network services and settings, including processes and related information, to be collected on-demand (or as scheduled). Windows packet captures are compiled in a proprietary eXtensible Markup Language (XML) format as "ETL" files (and associated "CAB" compressed files containing raw data), as shown in Figure 6-19 below. Any XML reader will suffice, but Microsoft also provides a free utility for reviewing the activity files,[202] as shown in Figure 6-20.



```
C:\Windows\system32>netsh trace start capture=yes Ethernet.Type=IPv4

Trace configuration:
-------------------------------------------------------------------
Status:             Running
Trace File:         C:\Users\[redacted]:\AppData\Local\Temp\NetTraces\NetTrace.etl
Append:             Off
Circular:           On
Max Size:           250 MB
Report:             Off

C:\Windows\system32>netsh trace stop
Correlating traces ... done
Generating data collection ... done
The trace file and additional troubleshooting information have been compiled as
"C:\Users\[redacted]:\AppData\Local\Temp\NetTraces\NetTrace.cab".
File location = C:\Users\[redacted]:\AppData\Local\Temp\NetTraces\NetTrace.etl
Tracing session was successfully stopped.

C:\Windows\system32>type c:\Users\[redacted]:\AppData\Local\Temp\NetTraces\netevents.
xml|more
ﾝ<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<netEvents numItems="312">
        <item>
                <header>
                        <timeStamp>2016-09-04T01:18:58.750Z</timeStamp>
                        <flags numItems="8">
                                <item>FWPM_NET_EVENT_FLAG_IP_PROTOCOL_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_LOCAL_ADDR_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_REMOTE_ADDR_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_LOCAL_PORT_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_REMOTE_PORT_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_APP_ID_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_USER_ID_SET</item>
                                <item>FWPM_NET_EVENT_FLAG_IP_VERSION_SET</item>
                        </flags>
                        <ipVersion>FWP_IP_VERSION_V4</ipVersion>
                        <ipProtocol>6</ipProtocol>
                        <localAddrV4>64.4.54.254</localAddrV4>
                        <remoteAddrV4>192.168.1.189</remoteAddrV4>
                        <localPort>443</localPort>
                        <remotePort>4491</remotePort>
                        <scopeId>0</scopeId>
                        <appId>
                                <data>5c0064006500760069006300650005c006800610072
0064006400690073006b0076006f006c0075006d00650033005c00770069006e0064006f00770073
005c0073007900730074006500d00330032005c007300760063068006f00730074002e00650078
0065000000</data>
                                <asString>\.d.e.v.i.c.e.\.h.a.r.d.d.i.s.k.v.o.l.
u.m.e.3.\.w.i.n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.s.v.c.h.o.s.t...e.x.e...</asString>
                        </appId>
                        <userId>S-1-5-19</userId>
                </header>
                <type>FWPM_NET_EVENT_TYPE_CLASSIFY_DROP</type>
-- More  --
```

Figure 6-19. Windows NETSH TRACE



teredo.ipv6.microsoft.com

Right click on any column header and select 'Group' to create a grouping.

Timestamp	EventRecord.Header.ProcessId	Module	Summary
2016-09-03T19:51:19.0518597	3748	TLS	Records: [ApplicationData(Encrypted)]
2016-09-03T19:51:18.3445387	0	TCP	Flags: ...A...., SrcPort: 5051, DstPort:
2016-09-03T19:51:18.0513510	3748	TLS	Records: [ApplicationData(Encrypted)]
2016-09-03T19:51:17.9633471	4	TLS	Records: [ApplicationData(Encrypted)]
2016-09-03T19:51:17.9126512	3748	TLS	Records: [ApplicationData(Encrypted), App
2016-09-03T19:51:17.8971836	3748	TLS	Records: [ApplicationData(Encrypted)]
2016-09-03T19:51:17.7944654	3748	TLS	Records: [ApplicationData(Encrypted)]
2016-09-03T19:51:21.6074231	1504	DNS	Request, Query ID: 0x7B9C, OpCode: QUERY,
2016-09-03T19:51:18.8888545	1596	UDP	SrcPort: 15892, DstPort: 58287, Length: 1
2016-09-03T19:51:24.4087776	9276	Windows_Kernel_Trace	Process_TypeGroup1{UniqueProcessKey=EtwPr
2016-09-03T19:51:24.4087758	9276	Windows_Kernel_Trace	Process_TypeGroup1{UniqueProcessKey=EtwPr

58 : DNS
Request, Query ID: 0x7B0C, OpCode: QUERY, C

58 : UDP
SrcPort: 57059, DstPort: DNS(53), Length: 51

58 : IPv4
Next Protocol: UDP, Packet ID: 5387, Total Lengt

58 : SNAP

Name	Value
Question	[Name: teredo.ipv6.microsoft.com, Ty
[0]	Name: teredo.ipv6.microsoft.com, Type
QueryName	teredo.ipv6.microsoft.com
Type	A(1) (0x0001)
Class	Internet(1) (0x0001)

58: Request, Query ID: 0x7B9C, OpCode: QUERY, Query Name: teredo.ipv6.micro

Name: teredo.ipv6.microsoft.com, Type: A, Class: Internet

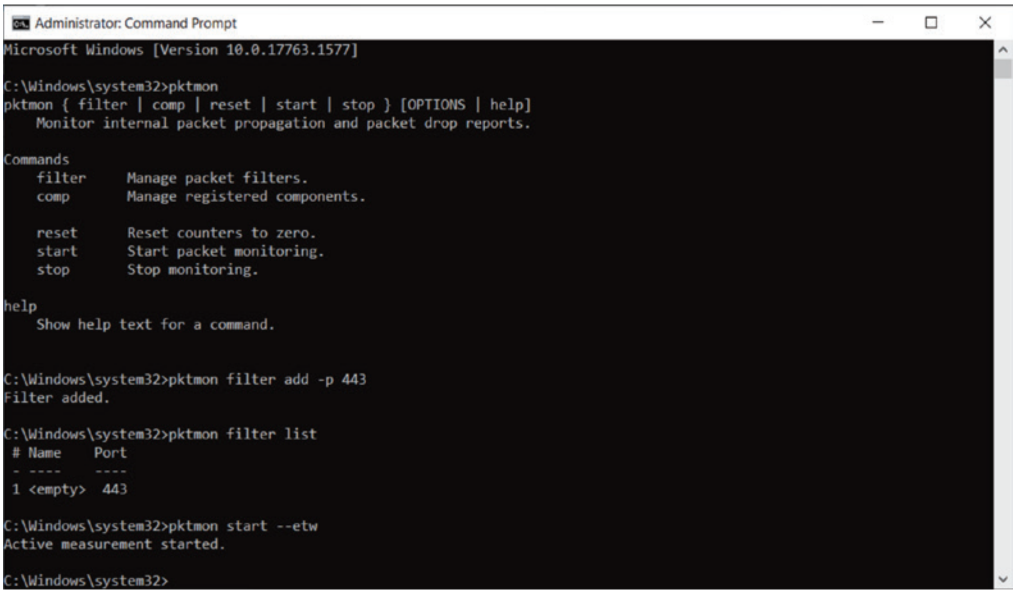
No alternate presentation available.

Ready   Session Total: 819   Available: 777   Selected: 1   Viewpoint: Default   Truncated Session: False   Build: 4.0.8108.0

Figure 6-20. Microsoft Analyzer for NETSH TRACE

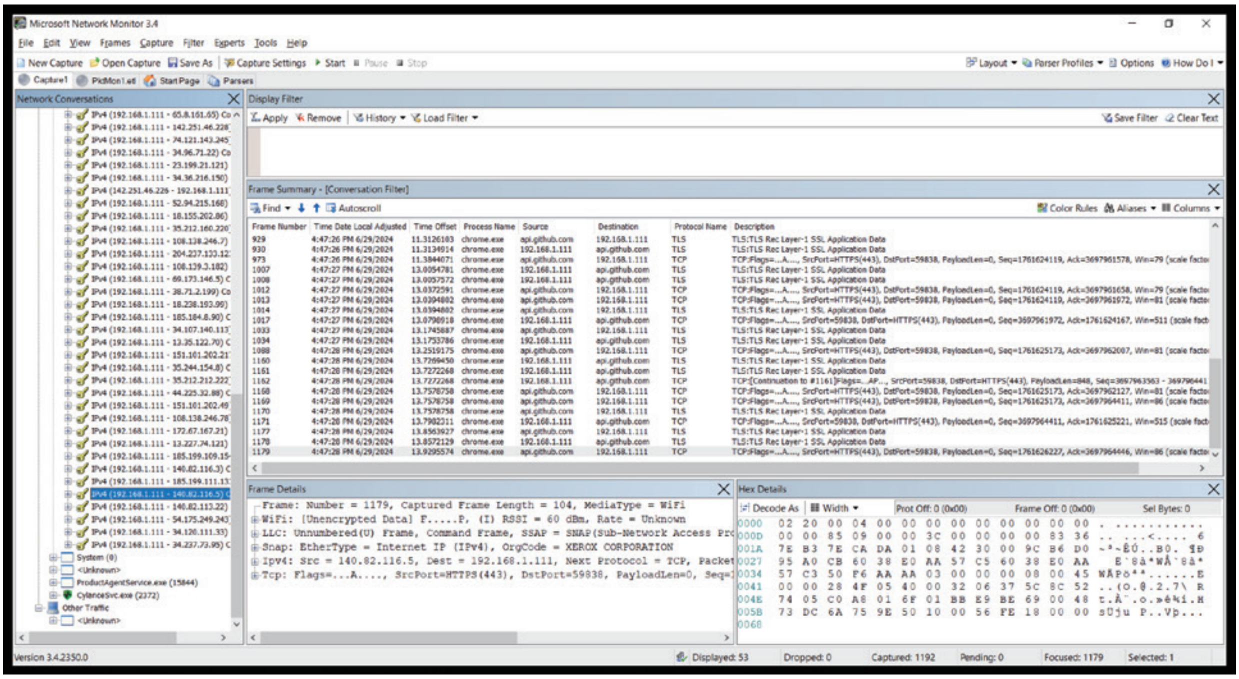
[202] https://www.microsoft.com/en-us/download/details.aspx?id=44226

The NETSH Trace utility in Windows was deprecated with the release of Windows 10, and a new utility called "PKTMON" was released. Once executed, pktmon will log all packets on ALL network interfaces on the device to a file called PktMon.etl and only record the first 128 bytes of a packet. To make it log the entire packet and only from a specific ethernet device, you can use the -p 0 (capture entire packet) and -c 13 (capture only from the adapter with ID 13) arguments. After stopping the capture a log file will be created in ETL format for review. A suitable viewer (Microsoft Network Monitor) or an ETL converter tool will be required.



```
Microsoft Windows [Version 10.0.17763.1577]

C:\Windows\system32>pktmon
pktmon { filter | comp | reset | start | stop } [OPTIONS | help]
    Monitor internal packet propagation and packet drop reports.

Commands
    filter      Manage packet filters.
    comp        Manage registered components.

    reset       Reset counters to zero.
    start       Start packet monitoring.
    stop        Stop monitoring.

help
    Show help text for a command.


C:\Windows\system32>pktmon filter add -p 443
Filter added.

C:\Windows\system32>pktmon filter list
 # Name     Port
 - ----     ----
 1 <empty>  443

C:\Windows\system32>pktmon start --etw
Active measurement started.

C:\Windows\system32>
```

Figure 6-20a. Microsoft PktMon.exe



```
IPv4 (192.168.1.111 - 65.8.161.65) Co
IPv4 (192.168.1.111 - 142.251.46.228
IPv4 (192.168.1.111 - 74.121.143.245
IPv4 (192.168.1.111 - 34.96.71.22) Co
IPv4 (192.168.1.111 - 23.199.21.121)
IPv4 (192.168.1.111 - 34.36.216.150)
IPv4 (142.251.46.226 - 192.168.1.111
IPv4 (192.168.1.111 - 52.94.215.168)
IPv4 (192.168.1.111 - 18.155.202.86)
IPv4 (192.168.1.111 - 35.212.160.220
IPv4 (192.168.1.111 - 108.138.246.7)
IPv4 (192.168.1.111 - 204.237.133.12
IPv4 (192.168.1.111 - 108.139.3.182)
IPv4 (192.168.1.111 - 69.173.146.5) C
IPv4 (192.168.1.111 - 38.71.2.199) Co
IPv4 (192.168.1.111 - 18.238.193.99)
IPv4 (192.168.1.111 - 185.184.8.90) C
IPv4 (192.168.1.111 - 34.107.140.113
IPv4 (192.168.1.111 - 13.35.122.70) C
IPv4 (192.168.1.111 - 151.101.202.21
IPv4 (192.168.1.111 - 35.244.154.8) C
IPv4 (192.168.1.111 - 35.212.212.222
IPv4 (192.168.1.111 - 44.225.32.88) C
IPv4 (192.168.1.111 - 151.101.202.49
IPv4 (192.168.1.111 - 108.138.246.78
IPv4 (192.168.1.111 - 172.67.167.21)
IPv4 (192.168.1.111 - 13.227.74.121)
IPv4 (192.168.1.111 - 185.199.109.15
IPv4 (192.168.1.111 - 140.82.116.3) C
IPv4 (192.168.1.111 - 185.199.111.13
IPv4 (192.168.1.111 - 140.82.116.5) C
IPv4 (192.168.1.111 - 140.82.113.22)
IPv4 (192.168.1.111 - 54.175.249.243
IPv4 (192.168.1.111 - 34.120.111.33)
IPv4 (192.168.1.111 - 34.237.73.95) C
System (0)
<Unknown>
ProductAgentService.exe (15844)
CylanceSvc.exe (2372)
Other Traffic
<Unknown>
```

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
929	4:47:26 PM 6/29/2024	11.3126103	chrome.exe	api.github.com	192.168.1.111	TLS	TLS:TLS Rec Layer-1 SSL Application Data
930	4:47:26 PM 6/29/2024	11.3134914	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
973	4:47:26 PM 6/29/2024	11.3844071	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761624119, Ack=3697961578, Win=79 (scale facto
1007	4:47:27 PM 6/29/2024	13.0054781	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1008	4:47:27 PM 6/29/2024	13.0057572	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1012	4:47:27 PM 6/29/2024	13.0372591	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761624119, Ack=3697961658, Win=79 (scale facto
1013	4:47:27 PM 6/29/2024	13.0394802	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761624119, Ack=3697961972, Win=81 (scale facto
1014	4:47:27 PM 6/29/2024	13.0394802	chrome.exe	api.github.com	192.168.1.111	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1017	4:47:27 PM 6/29/2024	13.0798918	chrome.exe	192.168.1.111	api.github.com	TCP	TCP:Flags=...A...., SrcPort=59838, DstPort=HTTPS(443), PayloadLen=0, Seq=3697961972, Ack=1761624167, Win=511 (scale fact
1033	4:47:27 PM 6/29/2024	13.1745887	chrome.exe	api.github.com	192.168.1.111	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1034	4:47:27 PM 6/29/2024	13.1753786	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1088	4:47:28 PM 6/29/2024	13.2519175	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761625173, Ack=3697962007, Win=81 (scale facto
1160	4:47:28 PM 6/29/2024	13.7269450	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1161	4:47:28 PM 6/29/2024	13.7272268	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1162	4:47:28 PM 6/29/2024	13.7272268	chrome.exe	192.168.1.111	api.github.com	TCP	TCP:[Continuation to #1161]Flags=...AP..., SrcPort=59838, DstPort=HTTPS(443), PayloadLen=848, Seq=3697963563 - 369796441
1168	4:47:28 PM 6/29/2024	13.7578758	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761625173, Ack=3697962127, Win=81 (scale facto
1169	4:47:28 PM 6/29/2024	13.7578758	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761625173, Ack=3697964411, Win=86 (scale facto
1170	4:47:28 PM 6/29/2024	13.7578758	chrome.exe	api.github.com	192.168.1.111	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1171	4:47:28 PM 6/29/2024	13.7902311	chrome.exe	192.168.1.111	api.github.com	TCP	TCP:Flags=...A...., SrcPort=59838, DstPort=HTTPS(443), PayloadLen=0, Seq=3697964411, Ack=1761625221, Win=515 (scale fact
1177	4:47:28 PM 6/29/2024	13.8563927	chrome.exe	api.github.com	192.168.1.111	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1178	4:47:28 PM 6/29/2024	13.8572129	chrome.exe	192.168.1.111	api.github.com	TLS	TLS:TLS Rec Layer-1 SSL Application Data
1179	4:47:28 PM 6/29/2024	13.9295574	chrome.exe	api.github.com	192.168.1.111	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1761626227, Ack=3697964446, Win=86 (scale facto

```
Frame: Number = 1179, Captured Frame Length = 104, MediaType = WiFi
WiFi: [Unencrypted Data] F.....P, (I) RSSI = 60 dBm, Rate = Unknown
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network Access Prc
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 140.82.116.5, Dest = 192.168.1.111, Next Protocol = TCP, Packet
Tcp: Flags=...A...., SrcPort=HTTPS(443), DstPort=59838, PayloadLen=0, Seq=1
```

```
Prot Off: 0 (0x00)      Frame Off: 0 (0x00)      Sel Bytes: 0
0000  02 20 00 04 00 00 00 00 00 00 00 00 00  . ...........
000D  00 00 85 09 00 00 3C 00 00 00 00 83 36  .. ...<.... 6
001A  7E B3 7E CA DA 01 08 42 30 00 9C B6 D0  ~³~ÊÚ..B0. ¶Ð
0027  95 A0 CB 60 38 E0 AA 57 C5 60 38 E0 AA   Ë`8à*WÅ`8à*
0034  57 C3 50 F6 AA AA 03 00 00 00 08 00 45  WÃPö**......E
0041  00 00 28 4F 05 40 00 32 06 37 5C 8C 52  ..(O.@.2.7\ R
004E  74 05 C0 A8 01 6F 01 BB E9 BE 69 00 48  t.À¨.o.»é¾i.H
005B  73 DC 6A 75 9E 50 10 00 56 FE 18 00 00  sÜju P..Vþ...
0068
```

Version 3.4.2350.0   Displayed: 53   Dropped: 0   Captured: 1192   Pending: 0   Focused: 1179   Selected: 1

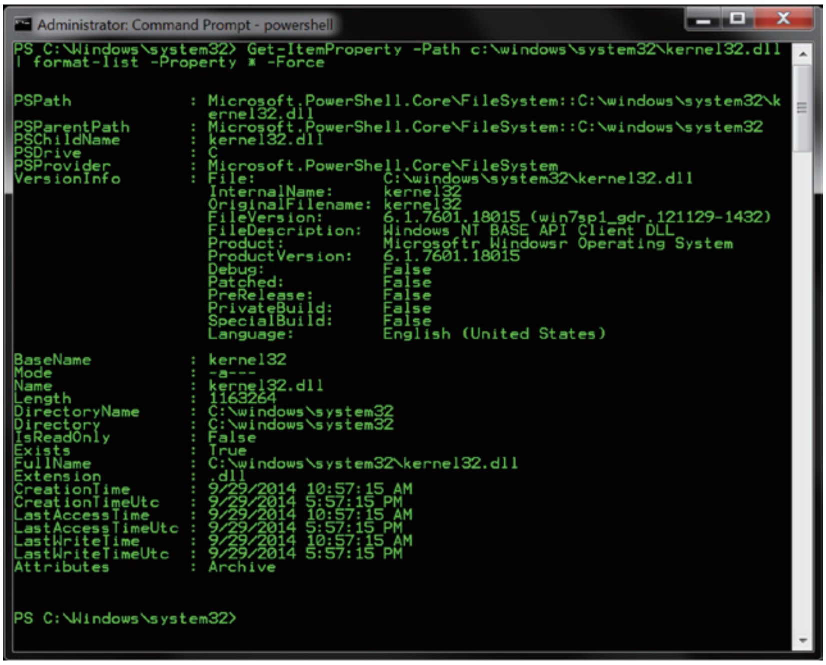
Figure 6-20b. Microsoft Network Monitor Conversion of PktMon1.etl

●Host Metadata

As previously described, metadata refers to "information about data". It does not contain contents of files but rather information about their content such as type, author, editor(s), created and modified (or deleted) dates and times, management privileges, sharing history, and related information about system and services including applications, configurations, and use history. Metadata is fundamentally important to collect as it helps investigators understand how a computer is configured and how it has been used, or how it relates to cybercrimes.

The simplest examples of host metadata have been demonstrated above with NET and PS API utilities. Many other similar tools such as "TASKMGR", "MSCONFIG or MSINFO32", "SCHTASKS", "AT", and "REG (QUERY)" provide important metadata artifacts that can be conveniently collected from Windows computers. Similar utilities exist in Linux and OSX as well. As described, these utilities essentially perform designed tasks that leverage APIs and scripting with native tools (PowerShell, .NET, VBScript, AutoIT, BASH, AWK, or etc.) and can accomplish the same tasks as well as facilitate custom outputs useful to the investigators' ETL format needs.

Investigators are primarily interested in file metadata. The file system history of creation, modification, last written, and deleted details for each file in their storage locations (and attributes that govern who has rights to the files) is important in identifying the crucial use (or misuse) history of a computer. Windows can provide some information from the "DIR" command, but it is limited by command flags for output and only returns "System Information" (SI) date/times rather than the more informative "Filesystem Note" (FN) date/time which is not modified by utilities that malware often employs to modify file creation dates. PowerShell can provide more complete detail (see Figure 6-21 below) and Visual Basic Scripts can return information from the FileSystem (FS) API.



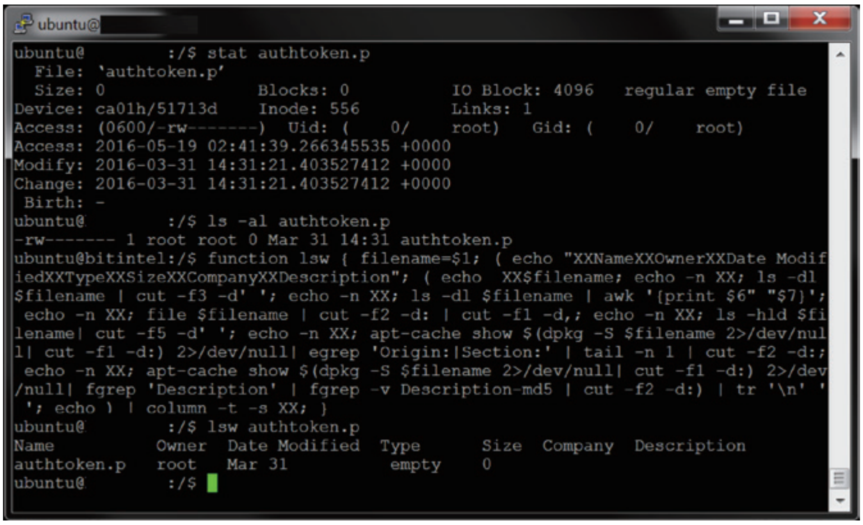
```
PS C:\Windows\system32> Get-ItemProperty -Path c:\windows\system32\kernel32.dll
| format-list -Property * -Force

PSPath            : Microsoft.PowerShell.Core\FileSystem::C:\windows\system32\k
                    ernel32.dll
PSParentPath      : Microsoft.PowerShell.Core\FileSystem::C:\windows\system32
PSChildName       : kernel32.dll
PSDrive           : C
PSProvider        : Microsoft.PowerShell.Core\FileSystem
VersionInfo       : File:             C:\windows\system32\kernel32.dll
                    InternalName:     kernel32
                    OriginalFilename: kernel32
                    FileVersion:      6.1.7601.18015 (win7sp1_gdr.121129-1432)
                    FileDescription:  Windows NT BASE API Client DLL
                    Product:          Microsoftr Windowsr Operating System
                    ProductVersion:   6.1.7601.18015
                    Debug:            False
                    Patched:          False
                    PreRelease:       False
                    PrivateBuild:     False
                    SpecialBuild:     False
                    Language:         English (United States)

BaseName          : kernel32
Mode              : -a---
Name              : kernel32.dll
Length            : 1163264
DirectoryName     : C:\windows\system32
Directory         : C:\windows\system32
IsReadOnly        : False
Exists            : True
FullName          : C:\windows\system32\kernel32.dll
Extension         : .dll
CreationTime      : 9/29/2014 10:57:15 AM
CreationTimeUtc   : 9/29/2014 5:57:15 PM
LastAccessTime    : 9/29/2014 10:57:15 AM
LastAccessTimeUtc : 9/29/2014 5:57:15 PM
LastWriteTime     : 9/29/2014 10:57:15 AM
LastWriteTimeUtc  : 9/29/2014 5:57:15 PM
Attributes        : Archive


PS C:\Windows\system32>
```

Figure 6-21. Windows PowerShell Filesystem Metadata

Linux and OSX can also provide relevant metadata, but several commands must be combined to gather coincidental artifact details. The "stat" command will return basic metadata about a file as will "ls -l", but a function can be programmed to combine varied metadata details into a single command[203]

[203] http://superuser.com/questions/554291/viewing-extended-file-properties-via-command-line-in-linux

that can be utilized for collection of evidence. See Figure 6-22 below for a snapshot of Linux metadata:



```
ubuntu@        :/$ stat authtoken.p
  File: 'authtoken.p'
  Size: 0               Blocks: 0          IO Block: 4096   regular empty file
Device: ca01h/51713d    Inode: 556         Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2016-05-19 02:41:39.266345535 +0000
Modify: 2016-03-31 14:31:21.403527412 +0000
Change: 2016-03-31 14:31:21.403527412 +0000
 Birth: -
ubuntu@        :/$ ls -al authtoken.p
-rw------- 1 root root 0 Mar 31 14:31 authtoken.p
ubuntu@bitintel:/$ function lsw { filename=$1; ( echo "XXNameXXOwnerXXDate Modif
iedXXTypeXXSizeXXCompanyXXDescription"; ( echo  XX$filename; echo -n XX; ls -dl
$filename | cut -f3 -d' '; echo -n XX; ls -dl $filename | awk '{print $6" "$7}';
 echo -n XX; file $filename | cut -f2 -d: | cut -f1 -d,; echo -n XX; ls -hld $fi
lename| cut -f5 -d' '; echo -n XX; apt-cache show $(dpkg -S $filename 2>/dev/nul
l| cut -f1 -d:) 2>/dev/null| egrep 'Origin:|Section:' | tail -n 1 | cut -f2 -d:;
 echo -n XX; apt-cache show $(dpkg -S $filename 2>/dev/null| cut -f1 -d:) 2>/dev
/null| fgrep 'Description' | fgrep -v Description-md5 | cut -f2 -d:) | tr '\n' '
 '; echo ) | column -t -s XX; }
ubuntu@        :/$ lsw authtoken.p
Name           Owner  Date Modified  Type      Size  Company  Description
authtoken.p    root   Mar 31          empty    0
ubuntu@        :/$ 
```

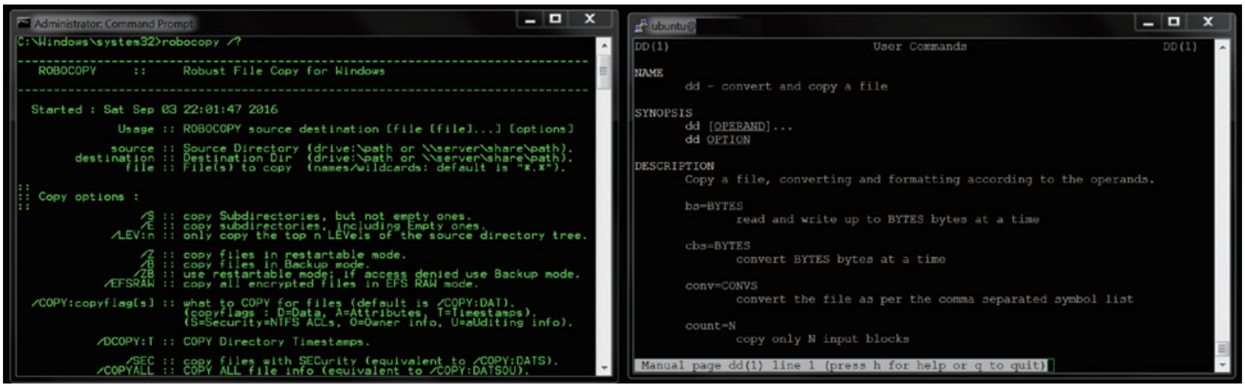
Figure 6-22. Linux lsw Metadata

Windows also includes a legacy utility called "Windows Management Interface Control" (WMIC)[204]. WMIC commands can return a wealth of details about systems including hardware, network, and application configurations and related details. For example, the "WMIC STARTUP" command will return commands and programs configured to run automatically when the computer is restarted. PowerShell, WMIC, and many Windows commands can also be used to access remote hosts to collect information.

●Host Files/Content

It is important to maintain the integrity of file contents so they can be relied upon as evidence. Standard "copy" utilities should be avoided when copying files for evidence collection, as they will modify signature details (metadata including the cryptographic hash value). Fortunately, Linux includes a basic forensic disk imaging utility that underlies nearly every third-party digital forensics utility– "disk duplicator" (dd). Windows also contains an API function that is utilized by similar utilities including backup software– "copy" (ccin/out is the function called). The copy function is somewhat confusing as it has the same name as the Windows "COPY.EXE" program which does not maintain the metadata properties. Conversely, Windows "ROBOCOPY.EXE" and "XCOPY.EXE" commands utilize the API properly. As such, it is generally recommended to use "dd" with Linux, and "ROBOCOPY /DATSOU" with Windows (see Figure 6-23 below). Note that for transportability the files should be compressed, and any time a file is collected a cryptographic hash signature should be calculated and documented.

[204] http://ss64.com/nt/wmic.html



```
C:\Windows\system32>robocopy /?

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows

-------------------------------------------------------------------------------

  Started : Sat Sep 03 22:01:47 2016

              Usage :: ROBOCOPY source destination [file [file]...] [options]

             source :: Source Directory (drive:\path or \\server\share\path).
        destination :: Destination Dir  (drive:\path or \\server\share\path).
               file :: File(s) to copy  (names/wildcards: default is "*.*").

::
:: Copy options :
::
                 /S :: copy Subdirectories, but not empty ones.
                 /E :: copy subdirectories, including Empty ones.
             /LEV:n :: only copy the top n LEVels of the source directory tree.

                 /Z :: copy files in restartable mode.
                 /B :: copy files in Backup mode.
                /ZB :: use restartable mode; if access denied use Backup mode.
            /EFSRAW :: copy all encrypted files in EFS RAW mode.

  /COPY:copyflag[s] :: what to COPY for files (default is /COPY:DAT).
                       (copyflags : D=Data, A=Attributes, T=Timestamps).
                       (S=Security=NTFS ACLs, O=Owner info, U=aUditing info).

           /DCOPY:T :: COPY Directory Timestamps.

               /SEC :: copy files with SECurity (equivalent to /COPY:DATS).
           /COPYALL :: COPY ALL file info (equivalent to /COPY:DATSOU).
```

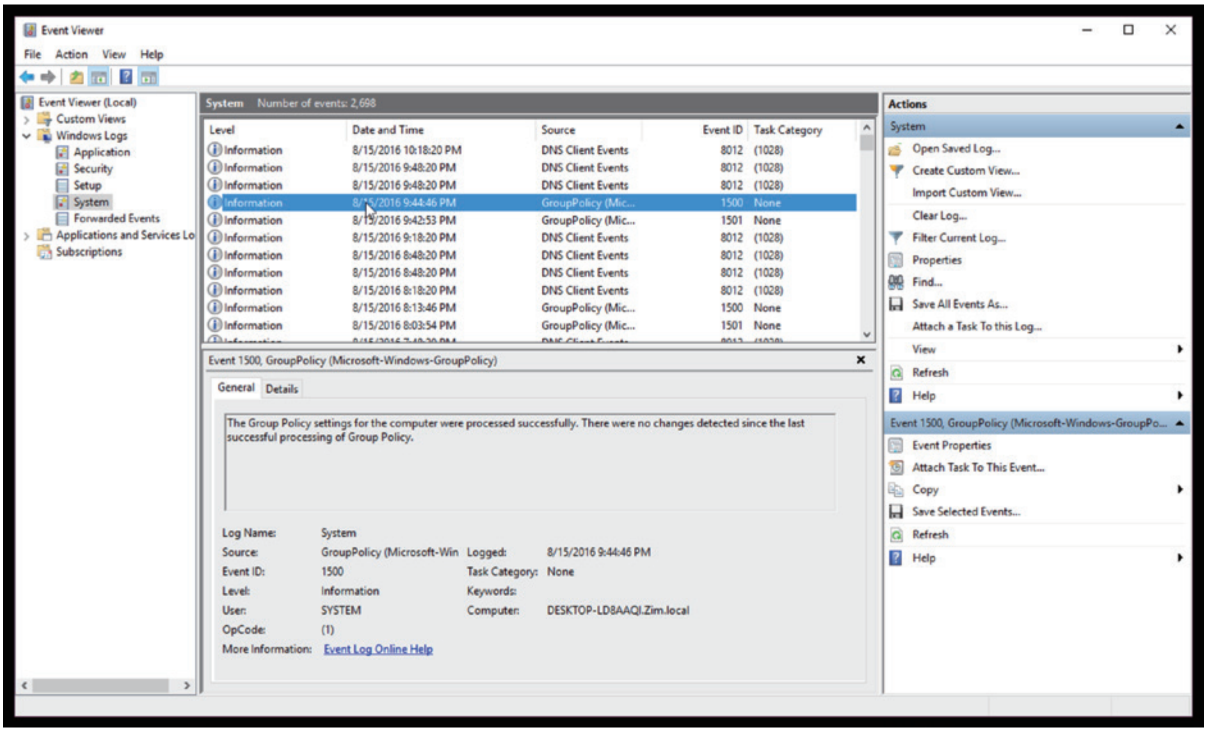
```
DD(1)                            User Commands                           DD(1)

NAME
       dd - convert and copy a file

SYNOPSIS
       dd [OPERAND]...
       dd OPTION

DESCRIPTION
       Copy a file, converting and formatting according to the operands.

       bs=BYTES
              read and write up to BYTES bytes at a time

       cbs=BYTES
              convert BYTES bytes at a time

       conv=CONVS
              convert the file as per the comma separated symbol list

       count=N
              copy only N input blocks

 Manual page dd(1) line 1 (press h for help or q to quit)
```

Figure 6-23. Windows ROBOCOPY and Linux dd

Certain files with content relevant to ascertaining a specific artifact' s relationship to a cybercrime may be locked by system operations and will not be accessible for copy operations. This includes master/journal file system information that contains the index of files by "inode" (attributes and disk block location). The commands previously mentioned can be used to parse information from locked files and ROBOCOPY/dd commands can facilitate other requirements. Useful third-party forensic copy utilities should be used in place of native commands for the collection of metadata artifacts specifically, including the locked file system logs, registry hives, and user configuration/history files. This will be discussed further in the "Third Party Tools" section below.

●Logs

Many applications create useful logs that are stored in various locations. These logs may be in proprietary formats or "normalized" (text or XML etc.) formats. Typically, third-party application log files will have ".LOG" or ".DB" extensions, or "LOG" in the name if on Linux or similar operating systems. Windows log files, however, use "Event" (EVT/EVTX) or "Data" (DAT) extensions and formats. These files can be extracted with native tools including "REG" for Data files and "WEVTUTIL" for Event logs. When collecting information from log files on live operating systems with native tools, it is necessary to either utilize the graphical applications (Windows Event Viewer or RegEdit- see Figure 6-24 below) to export data into a transportable format or to use suitable commands or scripting instructions to accomplish the same result.



System Number of events: 2,698

Level	Date and Time	Source	Event ID	Task Category
Information	8/15/2016 10:18:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 9:48:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 9:48:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 9:44:46 PM	GroupPolicy (Mic...	1500	None
Information	8/15/2016 9:42:53 PM	GroupPolicy (Mic...	1501	None
Information	8/15/2016 9:18:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 8:48:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 8:48:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 8:18:20 PM	DNS Client Events	8012	(1028)
Information	8/15/2016 8:13:46 PM	GroupPolicy (Mic...	1500	None
Information	8/15/2016 8:03:54 PM	GroupPolicy (Mic...	1501	None

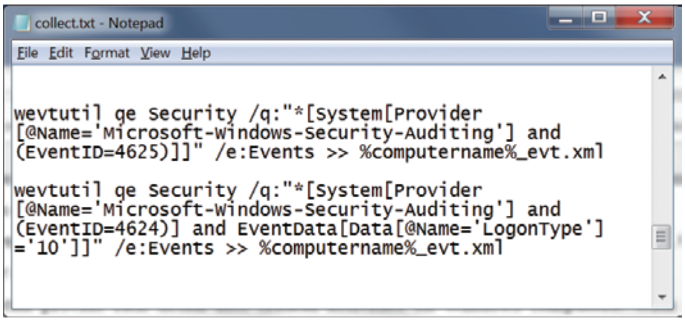
Event 1500, GroupPolicy (Microsoft-Windows-GroupPolicy)

The Group Policy settings for the computer were processed successfully. There were no changes detected since the last successful processing of Group Policy.

Log Name: System
Source: GroupPolicy (Microsoft-Win Logged: 8/15/2016 9:44:46 PM
Event ID: 1500 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-LD8AAQI.Zim.local
OpCode: (1)
More Information: Event Log Online Help

Figure 6-24. Windows Events Viewer

The following commands will return all failed logons to a Windows host and all successful remote desktop logons; both commands are configured to save the command outputs to a file:

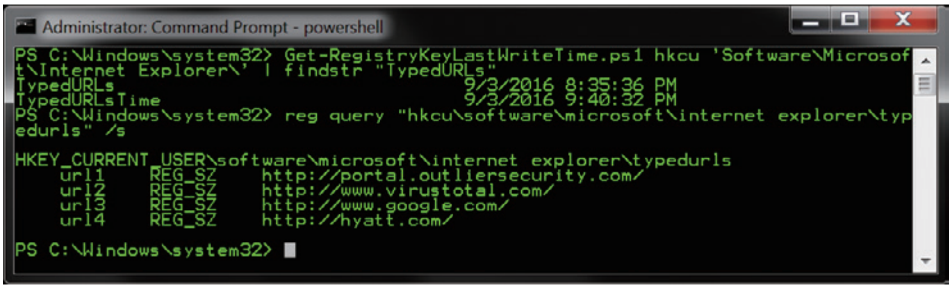


```
wevtutil qe Security /q:"*[System[Provider
[@Name='Microsoft-Windows-Security-Auditing'] and
(EventID=4625)]]" /e:Events >> %computername%_evt.xml

wevtutil qe Security /q:"*[System[Provider
[@Name='Microsoft-Windows-Security-Auditing'] and
(EventID=4624)] and EventData[Data[@Name='LogonType']
='10']]" /e:Events >> %computername%_evt.xml
```

Figure 6-25. Windows WEVTUTIL Query Utility

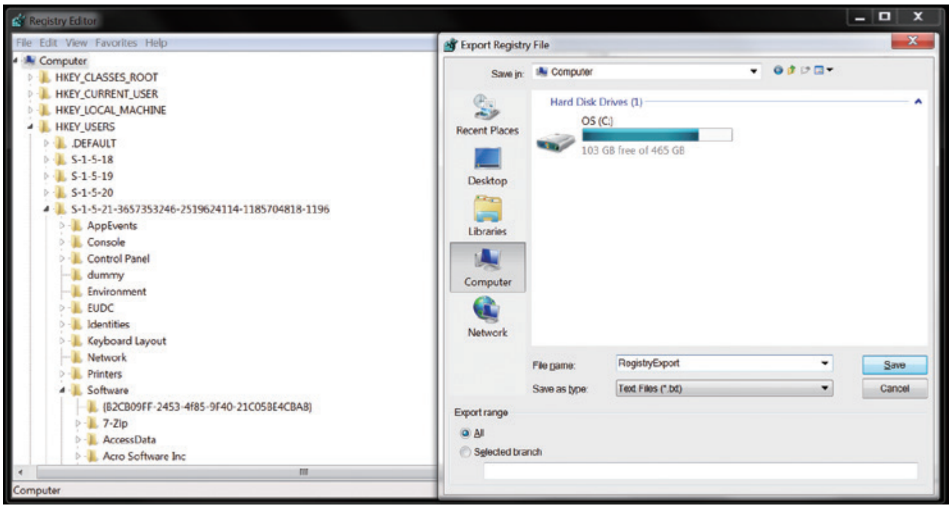
Linux typically saves logs in /var/log locations in normalized text formats. Simple “grep” or “cat” commands can be used to extract log details, though live log files can also be copied in Linux.

Windows Registry data files contain extensive information, but it can be challenging to collect it such that it contains enough literal data to assist analysts in determining timelines. A registry query or export command can return useful information such as services configurations or internet history, as shown below in Figures 6-26 and 6-27:



```
PS C:\Windows\system32> Get-RegistryKeyLastWriteTime.ps1 hkcu 'Software\Microsof
t\Internet Explorer\' | findstr "TypedURLs"
TypedURLs                               9/3/2016 8:35:36 PM
TypedURLsTime                           9/3/2016 9:40:32 PM
PS C:\Windows\system32> reg query "hkcu\software\microsoft\internet explorer\typ
edurls" /s

HKEY_CURRENT_USER\software\microsoft\internet explorer\typedurls
    url1    REG_SZ    http://portal.outliersecurity.com/
    url2    REG_SZ    http://www.virustotal.com/
    url3    REG_SZ    http://www.google.com/
    url4    REG_SZ    http://hyatt.com/

PS C:\Windows\system32> █
```

Figure 6-26. Windows TypedURL History



Save in: Computer

File name: RegistryExport

Save as type: Text Files (*.txt)

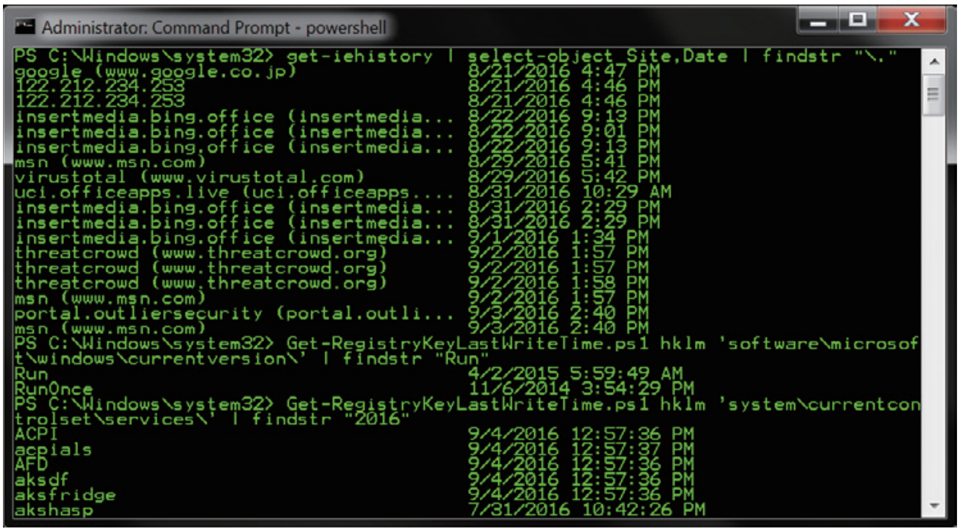
Export range

● All

○ Selected branch

Figure 6-27. Windows REGEDIT Export

Extracting date/time information requires more effort. PowerShell scripting can be a useful tool[205] and as mentioned can be utilized for the collection of local or remote host information in Windows networks:



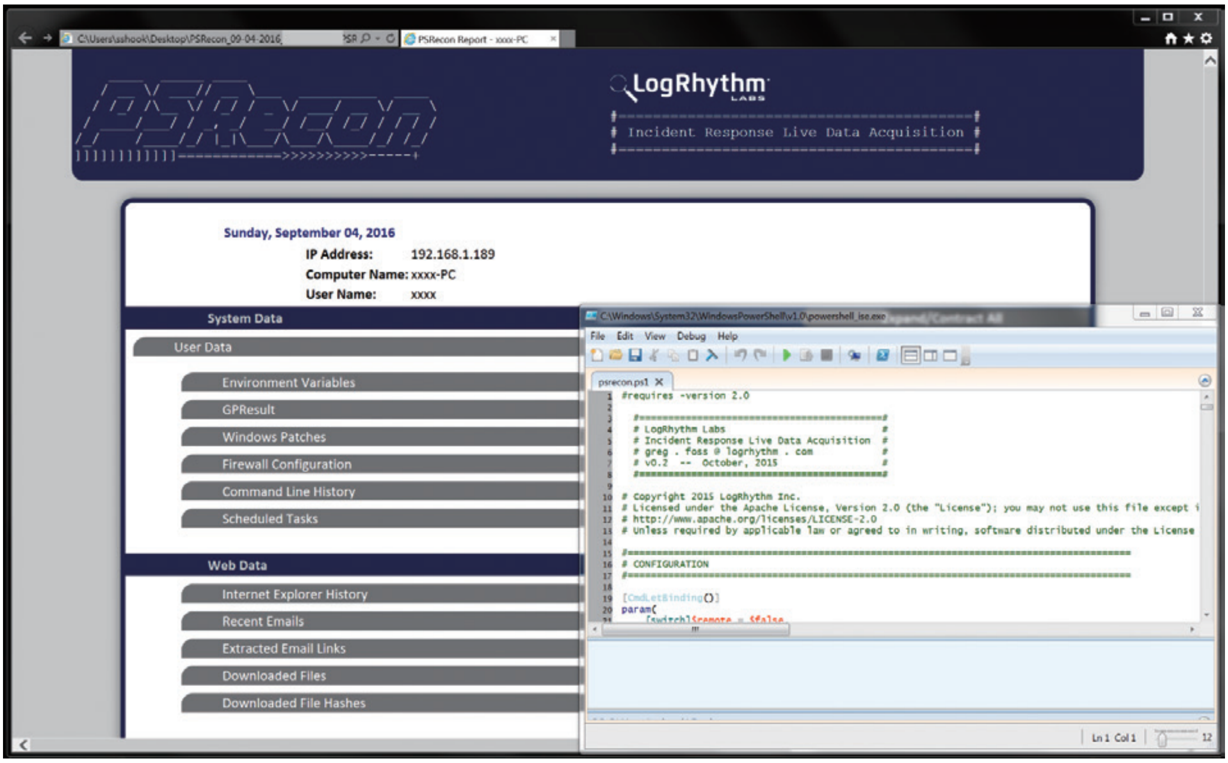
```
PS C:\Windows\system32> get-iehistory | select-object Site,Date | findstr "\."
google (www.google.co.jp)               8/21/2016 4:47 PM
122.212.234.253                         8/21/2016 4:46 PM
122.212.234.253                         8/21/2016 4:46 PM
insertmedia.bing.office (insertmedia... 8/22/2016 9:13 PM
insertmedia.bing.office (insertmedia... 8/22/2016 9:01 PM
insertmedia.bing.office (insertmedia... 8/22/2016 9:13 PM
msn (www.msn.com)                       8/29/2016 5:41 PM
virustotal (www.virustotal.com)         8/29/2016 5:42 PM
uci.officeapps.live (uci.officeapps.... 8/31/2016 10:29 AM
insertmedia.bing.office (insertmedia... 8/31/2016 2:29 PM
insertmedia.bing.office (insertmedia... 8/31/2016 2:29 PM
insertmedia.bing.office (insertmedia... 9/1/2016 1:34 PM
threatcrowd (www.threatcrowd.org)       9/2/2016 1:57 PM
threatcrowd (www.threatcrowd.org)       9/2/2016 1:57 PM
threatcrowd (www.threatcrowd.org)       9/2/2016 1:58 PM
msn (www.msn.com)                       9/2/2016 1:57 PM
portal.outliersecurity (portal.outli... 9/3/2016 2:40 PM
msn (www.msn.com)                       9/3/2016 2:40 PM
PS C:\Windows\system32> Get-RegistryKeyLastWriteTime.ps1 hklm 'software\microsof
t\windows\currentversion\' | findstr "Run"
Run                                     4/2/2015 5:59:49 AM
RunOnce                                 11/6/2014 3:54:29 PM
PS C:\Windows\system32> Get-RegistryKeyLastWriteTime.ps1 hklm 'system\currentcon
trolset\services\' | findstr "2016"
ACPI                                    9/4/2016 12:57:36 PM
acpials                                 9/4/2016 12:57:37 PM
AFD                                     9/4/2016 12:57:36 PM
aksdf                                   9/4/2016 12:57:36 PM
aksfridge                               9/4/2016 12:57:36 PM
akshasp                                 7/31/2016 10:42:26 PM
```

Figure 6-28. Windows PowerShell Examples

[205] https://gallery.technet.microsoft.com/scriptcenter/Get-RegistryKeyLastWriteTim-63f4dd96 and https://richardspowershellblog.wordpress.com/2011/06/29/ie-history-to-csv/

With the standardization of PowerShell in Windows since Windows 7 released (it was available in earlier versions but as an optional installation only) and with its recent release to support Linux, many useful methods of collecting evidence using native features of the operating system have been created. Two very good examples include PSRecon and Get-Memory-Dump.

PSRecon[206] uses several of the native techniques described above to collect host information (from a local or remote computer). It is designed for incident response but is also an effective manual collection utility. Although it is technically a third-party tool, it was released as free software under the "Apache" license[207]. The script provides very useful details about how to utilize native tools to collect evidence- see Figure 6-29 below:



C:\Users\sshook\Desktop\PSRecon_09-04-2016
PSRecon Report - xxxx-PC
LogRhythm LABS
# Incident Response Live Data Acquisition #

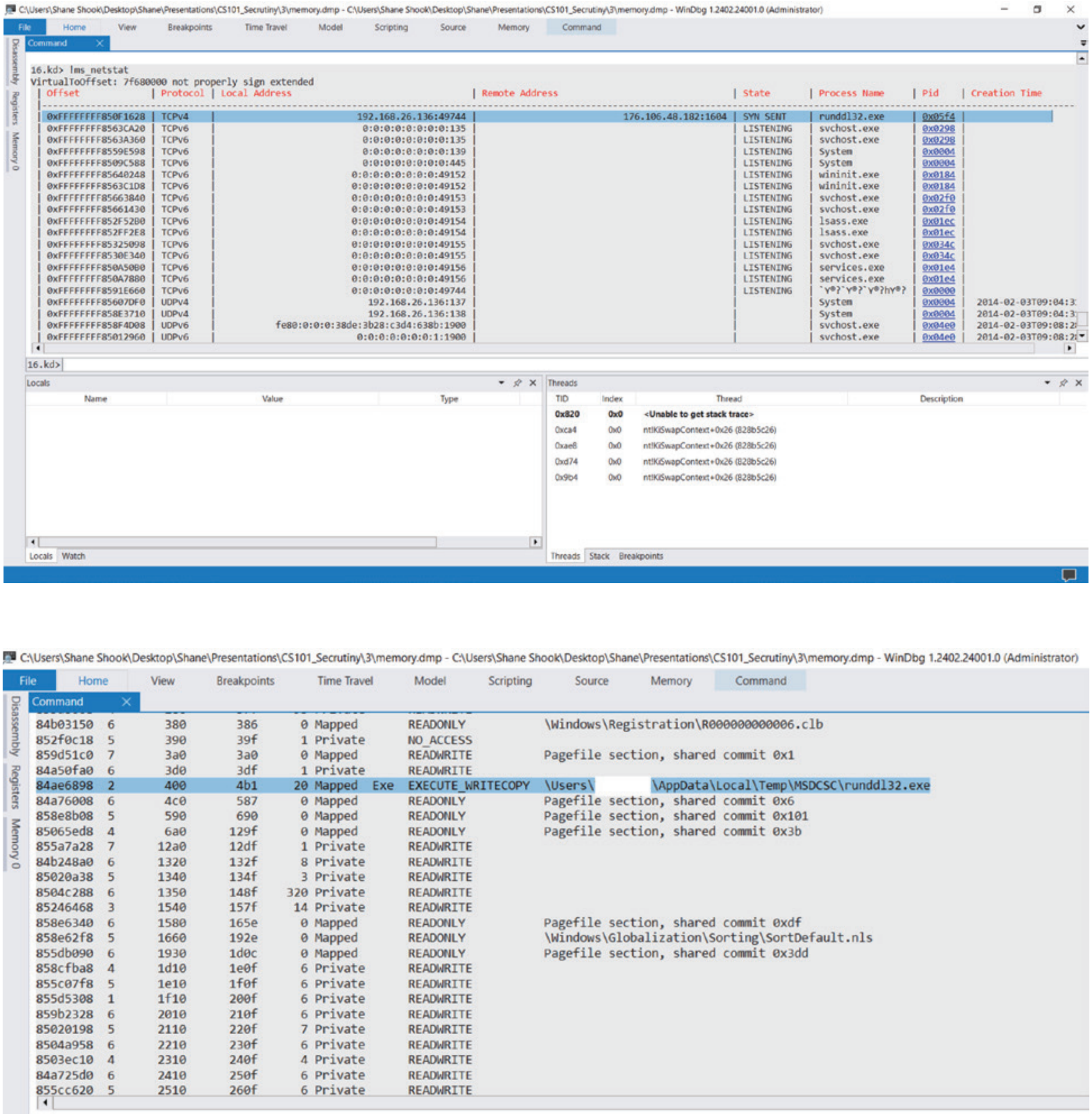
Sunday, September 04, 2016
IP Address: 192.168.1.189
Computer Name: xxxx-PC
User Name: xxxx

```
#requires -version 2.0

  #==========================================#
  # LogRhythm Labs                           #
  # Incident Response Live Data Acquisition  #
  # greg . foss @ logrhythm . com            #
  # v0.2  --  October, 2015                  #
  #==========================================#

# Copyright 2015 LogRhythm Inc.
# Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except i
# http://www.apache.org/licenses/LICENSE-2.0
# Unless required by applicable law or agreed to in writing, software distributed under the License

#==========================================================================================
# CONFIGURATION
#==========================================================================================

[CmdLetBinding()]
param(
    [switch]$remote = $false
```

Figure 6-29. PSRecon

Get-Memory-Dump[208] is a module released by Microsoft to allow live memory acquisition from Windows computers using the Microsoft Crash Dump format. Windows Debugger (WinDBG)[209] can be used to review the dump file and third-party tools like Volatility[210] can be used to extract information from the memory dump such as active process information, network information, user history, open files, and services configurations. These metadata, and actual file contents if the files are loaded into memory at the time of acquisition, can be collected simply and comprehensively from local or remote computers using PowerShell. Linux has similar access to produce memory dump files in /dev/(crash or mem). It is recommended to test these concepts before use.

[206] https://github.com/gfoss/PSRecon/blob/master/psrecon.ps1
[207] https://tldrlegal.com/license/apache-license-2.0-(apache-2.0)
[208] https://gallery.technet.microsoft.com/scriptcenter/Get-MemoryDump-c5ab38d8
[209] https://msdn.microsoft.com/en-us/library/windows/hardware/ff539316(v=vs.85).aspx
[210] http://www.volatilityfoundation.org/#!releases/component_71401



C:\Users\Shane Shook\Desktop\Shane\Presentations\CS101_Secrutiny\3\memory.dmp - C:\Users\Shane Shook\Desktop\Shane\Presentations\CS101_Secrutiny\3\memory.dmp - WinDbg 1.2402.24001.0 (Administrator)
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Source
Memory
Command
Command
Disassembly
Registers
Memory 0

```
16.kd> !ms_netstat
VirtualToOffset: 7f680000 not properly sign extended
 | Offset             | Protocol | Local Address                                | Remote Address                | State       | Process Name          | Pid    | Creation Time
 |-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 | 0xFFFFFFFF850F1628 | TCPv4    |                         192.168.26.136:49744 |          176.106.48.182:1604 | SYN SENT    | runddl32.exe          | 0x05f4 |
 | 0xFFFFFFFF8563CA20 | TCPv6    |                         0:0:0:0:0:0:0:0:135 |                               | LISTENING   | svchost.exe           | 0x0298 |
 | 0xFFFFFFFF8563A360 | TCPv6    |                         0:0:0:0:0:0:0:0:135 |                               | LISTENING   | svchost.exe           | 0x0298 |
 | 0xFFFFFFFF8559E598 | TCPv6    |                         0:0:0:0:0:0:0:0:139 |                               | LISTENING   | System                | 0x0004 |
 | 0xFFFFFFFF8509C588 | TCPv6    |                         0:0:0:0:0:0:0:0:445 |                               | LISTENING   | System                | 0x0004 |
 | 0xFFFFFFFF85640248 | TCPv6    |                       0:0:0:0:0:0:0:0:49152 |                               | LISTENING   | wininit.exe           | 0x0184 |
 | 0xFFFFFFFF8563C1D8 | TCPv6    |                       0:0:0:0:0:0:0:0:49152 |                               | LISTENING   | wininit.exe           | 0x0184 |
 | 0xFFFFFFFF85663840 | TCPv6    |                       0:0:0:0:0:0:0:0:49153 |                               | LISTENING   | svchost.exe           | 0x02f0 |
 | 0xFFFFFFFF85661430 | TCPv6    |                       0:0:0:0:0:0:0:0:49153 |                               | LISTENING   | svchost.exe           | 0x02f0 |
 | 0xFFFFFFFF852F52B0 | TCPv6    |                       0:0:0:0:0:0:0:0:49154 |                               | LISTENING   | lsass.exe             | 0x01ec |
 | 0xFFFFFFFF852FF2E8 | TCPv6    |                       0:0:0:0:0:0:0:0:49154 |                               | LISTENING   | lsass.exe             | 0x01ec |
 | 0xFFFFFFFF85325098 | TCPv6    |                       0:0:0:0:0:0:0:0:49155 |                               | LISTENING   | svchost.exe           | 0x034c |
 | 0xFFFFFFFF8530E340 | TCPv6    |                       0:0:0:0:0:0:0:0:49155 |                               | LISTENING   | svchost.exe           | 0x034c |
 | 0xFFFFFFFF850A50B0 | TCPv6    |                       0:0:0:0:0:0:0:0:49156 |                               | LISTENING   | services.exe          | 0x01e4 |
 | 0xFFFFFFFF850A7880 | TCPv6    |                       0:0:0:0:0:0:0:0:49156 |                               | LISTENING   | services.exe          | 0x01e4 |
 | 0xFFFFFFFF8591E660 | TCPv6    |                       0:0:0:0:0:0:0:0:49744 |                               | LISTENING   | `Y®?`Y®?`Y®?hY®?      | 0x0000 |
 | 0xFFFFFFFF85607DF0 | UDPv4    |                          192.168.26.136:137 |                               |             | System                | 0x0004 | 2014-02-03T09:04:3
 | 0xFFFFFFFF858E3710 | UDPv4    |                          192.168.26.136:138 |                               |             | System                | 0x0004 | 2014-02-03T09:04:3
 | 0xFFFFFFFF858F4D08 | UDPv6    |        fe80:0:0:0:38de:3b28:c3d4:638b:1900 |                               |             | svchost.exe           | 0x04e0 | 2014-02-03T09:08:2
 | 0xFFFFFFFF85012960 | UDPv6    |                       0:0:0:0:0:0:0:1:1900 |                               |             | svchost.exe           | 0x04e0 | 2014-02-03T09:08:2
16.kd>
```

Threads

TID	Index	Thread	Description
0x820	**0x0**	**<Unable to get stack trace>**	
0xca4	0x0	nt!KiSwapContext+0x26 (828b5c26)	
0xae8	0x0	nt!KiSwapContext+0x26 (828b5c26)	
0xd74	0x0	nt!KiSwapContext+0x26 (828b5c26)	
0x9b4	0x0	nt!KiSwapContext+0x26 (828b5c26)	

C:\Users\Shane Shook\Desktop\Shane\Presentations\CS101_Secrutiny\3\memory.dmp - C:\Users\Shane Shook\Desktop\Shane\Presentations\CS101_Secrutiny\3\memory.dmp - WinDbg 1.2402.24001.0 (Administrator)
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Source
Memory
Command
Command
Disassembly
Registers
Memory 0

```
84b03150  6    380    386    0 Mapped        READONLY           \Windows\Registration\R000000000006.clb
852f0c18  5    390    39f    1 Private       NO_ACCESS
859d51c0  7    3a0    3a0    0 Mapped        READWRITE          Pagefile section, shared commit 0x1
84a50fa0  6    3d0    3df    1 Private       READWRITE
84ae6898  2    400    4b1   20 Mapped   Exe  EXECUTE_WRITECOPY  \Users\        \AppData\Local\Temp\MSDCSC\rundd132.exe
84a76008  6    4c0    587    0 Mapped        READONLY           Pagefile section, shared commit 0x6
858e8b08  5    590    690    0 Mapped        READONLY           Pagefile section, shared commit 0x101
85065ed8  4    6a0    129f   0 Mapped        READONLY           Pagefile section, shared commit 0x3b
855a7a28  7    12a0   12df   1 Private       READWRITE
84b248a0  6    1320   132f   8 Private       READWRITE
85020a38  5    1340   134f   3 Private       READWRITE
8504c288  6    1350   148f 320 Private       READWRITE
85246468  3    1540   157f  14 Private       READWRITE
858e6340  6    1580   165e   0 Mapped        READONLY           Pagefile section, shared commit 0xdf
858e62f8  5    1660   192e   0 Mapped        READONLY           \Windows\Globalization\Sorting\SortDefault.nls
855db090  6    1930   1d0c   0 Mapped        READONLY           Pagefile section, shared commit 0x3dd
858cfba8  4    1d10   1e0f   6 Private       READWRITE
855c07f8  5    1e10   1f0f   6 Private       READWRITE
855d5308  1    1f10   200f   6 Private       READWRITE
859b2328  6    2010   210f   6 Private       READWRITE
85020198  5    2110   220f   7 Private       READWRITE
8504a958  6    2210   230f   6 Private       READWRITE
8503ec10  4    2310   240f   4 Private       READWRITE
84a725d0  6    2410   250f   6 Private       READWRITE
855cc620  5    2510   260f   6 Private       READWRITE
```

Figure 6-29a. WinDBG (using SwishDbgExt.dll[211] for memory dump analysis)

Third-Party Tools

As described above, native tools can facilitate many incidental artifacts when collecting evidence of cybercrimes. Focused collection can also be achieved by leveraging native operating system APIs with the scripting utilities that exist on every endpoint– if the examiner performing the acquisition understands where, when, and how to use the APIs effectively. In place of those native methods of collecting artifacts and evidence, many third-party tools that leverage the same (or package similar) APIs can simplify evidence collection.

[211] https://github.com/MagnetForensics/SwishDbgExt

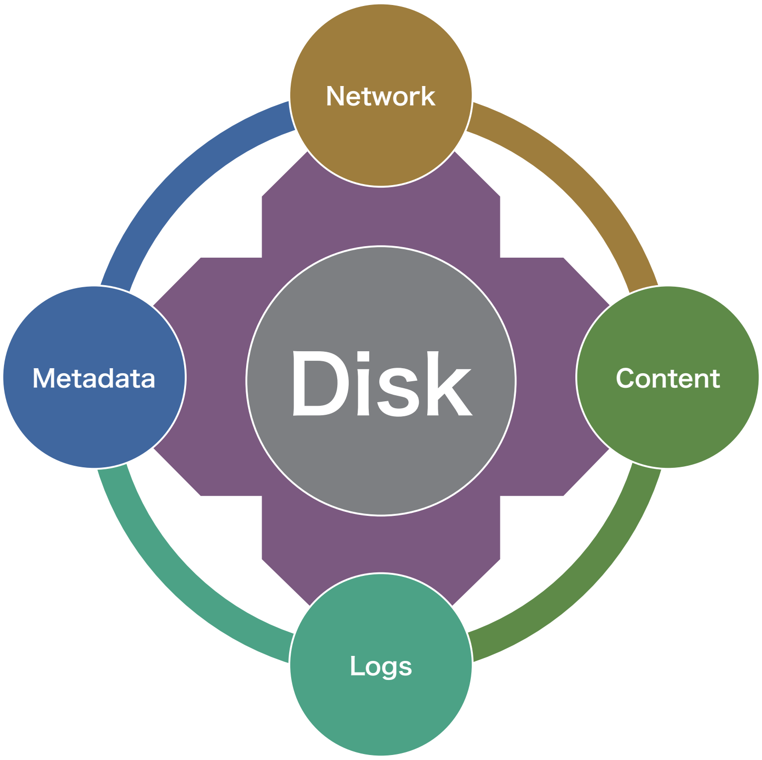


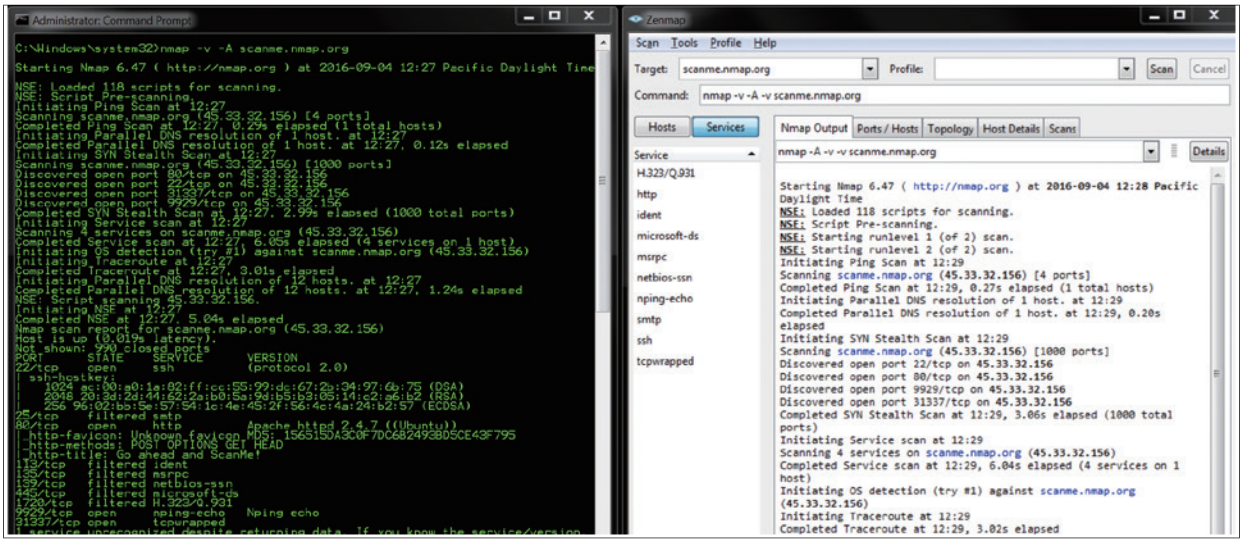
Figure 6-30. Investigator's Collection

Third-party tools often provide speed, convenience, and the benefits of community use such as modifications and feature requests. This section provides some examples of third-party tools that are commonly used in investigations and may be suitable to produce evidence in legal proceedings if necessary.

●Network

Network information can be gathered by tools such as NetworkMiner[212], nmap[213], tcpview[214], and WireShark[215]. "Network Mapper" (nmap) is an open-source tool that enables scanning of a host or a specified network by address or range. Nmap does not produce netflows but will list externally identified services configurations and host information. Nmap runs either as an application from the command line or graphically in different operating systems. See Figure 6-31 below:

[212] https://www.netresec.com/?page=NetworkMiner
[213] https://nmap.org/
[214] https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx
[215] https://www.wireshark.org/



```
C:\Windows\system32>nmap -v -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2016-09-04 12:27 Pacific Daylight Time

NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 12:27
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 12:27, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:27
Completed Parallel DNS resolution of 1 host. at 12:27, 0.12s elapsed
Initiating SYN Stealth Scan at 12:27
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Completed SYN Stealth Scan at 12:27, 2.99s elapsed (1000 total ports)
Initiating Service scan at 12:27
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 12:27, 6.05s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)
Initiating Traceroute at 12:27
Completed Traceroute at 12:27, 3.01s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:27
Completed Parallel DNS resolution of 12 hosts. at 12:27, 1.24s elapsed
NSE: Script scanning 45.33.32.156.
Initiating NSE at 12:27
Completed NSE at 12:27, 5.04s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.019s latency).
Not shown: 990 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          (protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795
|_http-methods: POST OPTIONS GET HEAD
|_http-title: Go ahead and ScanMe!
113/tcp   filtered ident
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1720/tcp  filtered H.323/Q.931
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
1 service unrecognized despite returning data. If you know the service/version
```

Target: scanme.nmap.org

Profile:

Command: nmap -v -A -v scanme.nmap.org

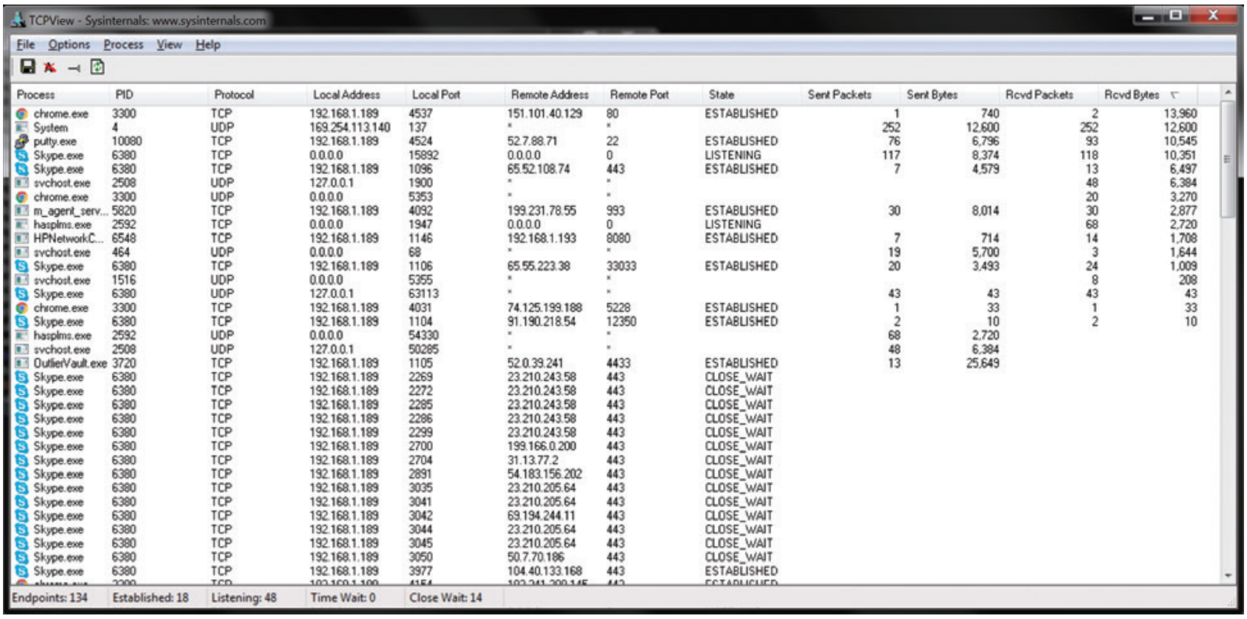
Service: H.323/Q.931, http, ident, microsoft-ds, msrpc, netbios-ssn, nping-echo, smtp, ssh, tcpwrapped

nmap -A -v -v scanme.nmap.org

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-09-04 12:28 Pacific
Daylight Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Initiating Ping Scan at 12:29
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 12:29, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:29
Completed Parallel DNS resolution of 1 host. at 12:29, 0.20s
elapsed
Initiating SYN Stealth Scan at 12:29
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 12:29, 3.06s elapsed (1000 total
ports)
Initiating Service scan at 12:29
Scanning 4 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 12:29, 6.04s elapsed (4 services on 1
host)
Initiating OS detection (try #1) against scanme.nmap.org
(45.33.32.156)
Initiating Traceroute at 12:29
Completed Traceroute at 12:29, 3.02s elapsed
```

Figure 6-31. NMAP

TCPView is similar to a combination of process and network API tools found in Windows and Linux. It was written by Mark Russinovich, the author of the extraordinarily popular "SysInternals Suite" [216] of tools that Microsoft added to their own products in 2016. TCPView is similar to the same-named utility from BSD Unix that was also ported to Solaris and various other Unix-based operating systems[217]. It simplifies the results of the "tcpdump" (and NETSH TRACE) outputs previously discussed:



TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
chrome.exe	3300	TCP	192.168.1.189	4537	151.101.40.129	80	ESTABLISHED	1	740	2	13,960
System	4	UDP	169.254.113.140	137	*	*		252	12,600	252	12,600
putty.exe	10080	TCP	192.168.1.189	4524	52.7.88.71	22	ESTABLISHED	76	6,796	93	10,545
Skype.exe	6380	TCP	0.0.0.0	15892	0.0.0.0	0	LISTENING	117	8,374	118	10,351
Skype.exe	6380	TCP	192.168.1.189	1096	65.52.108.74	443	ESTABLISHED	7	4,579	13	6,497
svchost.exe	2508	UDP	127.0.0.1	1900	*	*				48	6,384
chrome.exe	3300	UDP	0.0.0.0	5353	*	*				20	3,270
m_agent_serv...	5820	TCP	192.168.1.189	4092	199.231.78.55	993	ESTABLISHED	30	8,014	30	2,877
hasplms.exe	2592	TCP	0.0.0.0	1947	0.0.0.0	0	LISTENING			68	2,720
HPNetworkC...	6548	TCP	192.168.1.189	1146	192.168.1.193	8080	ESTABLISHED	7	714	14	1,708
svchost.exe	464	UDP	0.0.0.0	68	*	*		19	5,700	3	1,644
Skype.exe	6380	TCP	192.168.1.189	1106	65.55.223.38	33033	ESTABLISHED	20	3,493	24	1,009
svchost.exe	1516	UDP	0.0.0.0	5355	*	*				8	208
Skype.exe	6380	UDP	127.0.0.1	63113	*	*		43	43	43	43
chrome.exe	3300	TCP	192.168.1.189	4031	74.125.199.188	5228	ESTABLISHED	1	33	1	33
Skype.exe	6380	TCP	192.168.1.189	1104	91.190.218.54	12350	ESTABLISHED	2	10	2	10
hasplms.exe	2592	UDP	0.0.0.0	54330	*	*		68	2,720		
svchost.exe	2508	UDP	127.0.0.1	50285	*	*		48	6,384		
OutlierVault.exe	3720	TCP	192.168.1.189	1105	52.0.39.241	4433	ESTABLISHED	13	25,649		
Skype.exe	6380	TCP	192.168.1.189	2269	23.210.243.58	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2272	23.210.243.58	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2285	23.210.243.58	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2286	23.210.243.58	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2299	23.210.243.58	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2700	199.166.0.200	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2704	31.13.77.2	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	2891	54.183.156.202	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3035	23.210.205.64	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3041	23.210.205.64	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3042	69.194.244.11	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3044	23.210.205.64	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3045	23.210.205.64	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3050	50.7.70.186	443	CLOSE_WAIT				
Skype.exe	6380	TCP	192.168.1.189	3977	104.40.133.168	443	ESTABLISHED				
chrome.exe	3300	TCP	192.168.1.189	4154	192.241.200.145	443	ESTABLISHED				

Endpoints: 134 | Established: 18 | Listening: 48 | Time Wait: 0 | Close Wait: 14

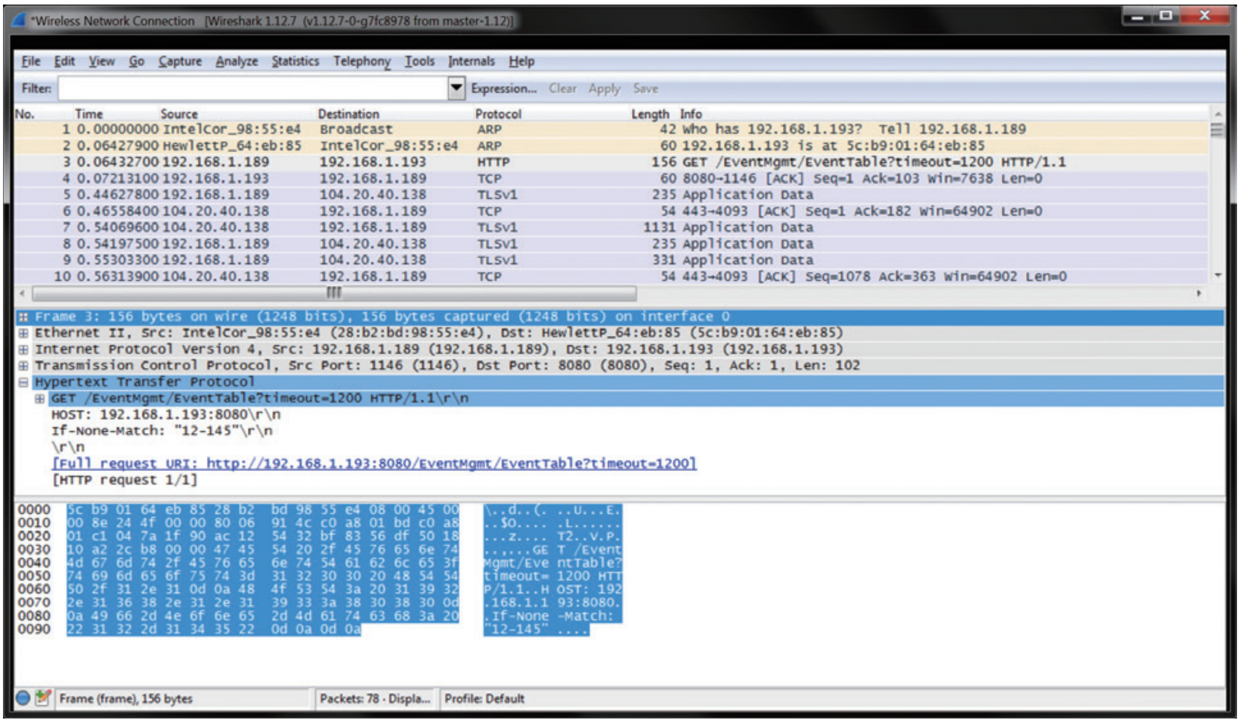
Figure 6-32. TCPView

Wireshark is also similar to tcpdump, but unlike TCPView, Wireshark will also capture full (or limited by specified commands) network packets and connection information. Wireshark uses the

[216] https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

[217] Linux have varied implementations of TCPView or similar utilities like NetActView or iftop etc.; however, a simple "lsof -i" command will return similar information that TCPView provides.

Packet Capture Library (libpcap)[218] which is also ported for Windows as WinPCAP[219]. Wireshark can be used by investigators to capture and analyze many diverse source formats, protocols, and content types in communications, either visually or programmatically. Files that are transferred between computers monitored with Wireshark or that are contained in tcpdump or other network packet capture files can be extracted with full content, according to whether the packet capture was configured to collect content details as well as connection metadata. Many other open-source and proprietary free or for-profit software are available to visualize and assist with tcpdump/PCAP analysis, but Wireshark contains the essential tools to collect network artifacts and related evidence:



*Wireless Network Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time        Source              Destination         Protocol   Length  Info
    1 0.00000000  IntelCor_98:55:e4   Broadcast           ARP            42  Who has 192.168.1.193?  Tell 192.168.1.189
    2 0.06427900  HewlettP_64:eb:85   IntelCor_98:55:e4   ARP            60  192.168.1.193 is at 5c:b9:01:64:eb:85
    3 0.06432700  192.168.1.189       192.168.1.193       HTTP          156  GET /EventMgmt/EventTable?timeout=1200 HTTP/1.1
    4 0.07213100  192.168.1.193       192.168.1.189       TCP            60  8080→1146 [ACK] Seq=1 Ack=103 Win=7638 Len=0
    5 0.44627800  192.168.1.189       104.20.40.138       TLSv1         235  Application Data
    6 0.46558400  104.20.40.138       192.168.1.189       TCP            54  443→4093 [ACK] Seq=1 Ack=182 Win=64902 Len=0
    7 0.54069600  104.20.40.138       192.168.1.189       TLSv1        1131  Application Data
    8 0.54197500  192.168.1.189       104.20.40.138       TLSv1         235  Application Data
    9 0.55303300  192.168.1.189       104.20.40.138       TLSv1         331  Application Data
   10 0.56313900  104.20.40.138       192.168.1.189       TCP            54  443→4093 [ACK] Seq=1078 Ack=363 Win=64902 Len=0
```

```
⊞ Frame 3: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_98:55:e4 (28:b2:bd:98:55:e4), Dst: HewlettP_64:eb:85 (5c:b9:01:64:eb:85)
⊞ Internet Protocol Version 4, Src: 192.168.1.189 (192.168.1.189), Dst: 192.168.1.193 (192.168.1.193)
⊞ Transmission Control Protocol, Src Port: 1146 (1146), Dst Port: 8080 (8080), Seq: 1, Ack: 1, Len: 102
⊟ Hypertext Transfer Protocol
  ⊞ GET /EventMgmt/EventTable?timeout=1200 HTTP/1.1\r\n
    HOST: 192.168.1.193:8080\r\n
    If-None-Match: "12-145"\r\n
    \r\n
    [Full request URI: http://192.168.1.193:8080/EventMgmt/EventTable?timeout=1200]
    [HTTP request 1/1]
```

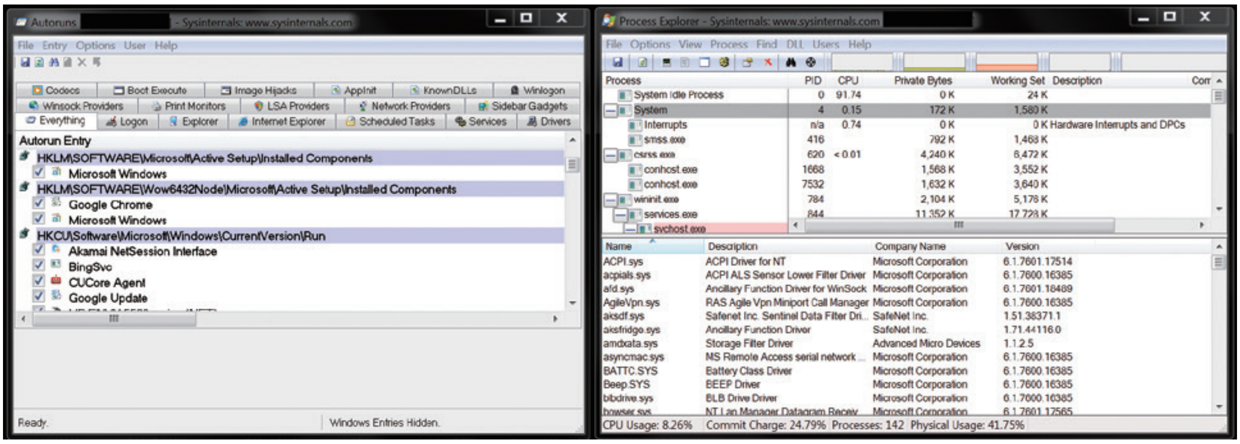
```
0000  5c b9 01 64 eb 85 28 b2  bd 98 55 e4 08 00 45 00   \..d..(. ..U...E.
0010  00 8e 24 4f 00 00 80 06  91 4c c0 a8 01 bd c0 a8   ..$O.... .L......
0020  01 c1 04 7a 1f 90 ac 12  54 32 bf 83 56 df 50 18   ...z.... T2..V.P.
0030  10 a2 2c b8 00 00 47 45  54 20 2f 45 76 65 6e 74   ..,...GE T /Event
0040  4d 67 6d 74 2f 45 76 65  6e 74 54 61 62 6c 65 3f   Mgmt/Eve ntTable?
0050  74 69 6d 65 6f 75 74 3d  31 32 30 30 20 48 54 54   timeout= 1200 HTT
0060  50 2f 31 2e 31 0d 0a 48  4f 53 54 3a 20 31 39 32   P/1.1..H OST: 192
0070  2e 31 36 38 2e 31 2e 31  39 33 3a 38 30 38 30 0d   .168.1.1 93:8080.
0080  0a 49 66 2d 4e 6f 6e 65  2d 4d 61 74 63 68 3a 20   .If-None -Match: 
0090  22 31 32 2d 31 34 35 22  0d 0a 0d 0a               "12-145" ....
```

Figure 6-33. Wireshark

●Host Metadata

A wide variety of tools exist to collect host metadata. The SysInternals Suite provides several utilities to gather information on open file handles, system configuration, running processes, autoruns, and more (see Figure 6-34 below). Host metadata collection, though, primarily involves the collection of Windows system files that are locked by operation on active systems including $MFT and $USNJrnl, operating system and user Registry Hives, Internet History, and Windows Event Logs. Special tools that allow local or remote collection of those metadata files for processing include RawCopy[220] and FGET[221] (see Figure 6-35 below).

[218] http://www.tcpdump.org/
[219] https://www.winpcap.org/
[220] https://github.com/jschicht/RawCopy
[221] http://opensecurityresearch.com/files/FGET.zip



Autorun Entry
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
☑ Microsoft Windows
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
☑ Google Chrome
☑ Microsoft Windows
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
☑ Akamai NetSession Interface
☑ BingSvc
☑ CUCore Agent
☑ Google Update

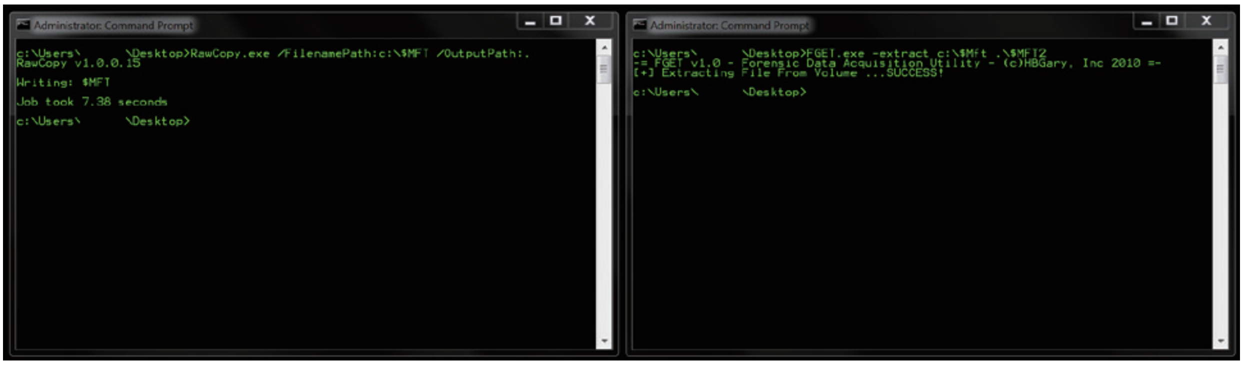
Ready. Windows Entries Hidden.

Process	PID	CPU	Private Bytes	Working Set	Description	Com
System Idle Process	0	91.74	0 K	24 K		
System	4	0.15	172 K	1,580 K		
Interrupts	n/a	0.74	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	416		792 K	1,468 K		
csrss.exe	620	< 0.01	4,240 K	6,472 K		
conhost.exe	1668		1,568 K	3,552 K		
conhost.exe	7532		1,632 K	3,640 K		
wininit.exe	784		2,104 K	5,176 K		
services.exe	844		11,352 K	17,728 K		
svchost.exe						

Name	Description	Company Name	Version
ACPI.sys	ACPI Driver for NT	Microsoft Corporation	6.1.7601.17514
acpials.sys	ACPI ALS Sensor Lower Filter Driver	Microsoft Corporation	6.1.7600.16385
afd.sys	Ancillary Function Driver for WinSock	Microsoft Corporation	6.1.7601.18489
AgileVpn.sys	RAS Agile Vpn Miniport Call Manager	Microsoft Corporation	6.1.7600.16385
aksdf.sys	Safenet Inc. Sentinel Data Filter Dri...	SafeNet Inc.	1.51.38371.1
aksfridge.sys	Ancillary Function Driver	SafeNet Inc.	1.71.44116.0
amdxata.sys	Storage Filter Driver	Advanced Micro Devices	1.1.2.5
asyncmac.sys	MS Remote Access serial network ...	Microsoft Corporation	6.1.7600.16385
BATTC.SYS	Battery Class Driver	Microsoft Corporation	6.1.7600.16385
Beep.SYS	BEEP Driver	Microsoft Corporation	6.1.7600.16385
blbdrive.sys	BLB Drive Driver	Microsoft Corporation	6.1.7600.16385
bowser.sys	NT Lan Manager Datagram Receiv	Microsoft Corporation	6.1.7601.17565

CPU Usage: 8.26% Commit Charge: 24.79% Processes: 142 Physical Usage: 41.75%

Figure 6-34. Autoruns and ProcExp



```
c:\Users\        \Desktop>RawCopy.exe /FilenamePath:c:\$MFT /OutputPath:.
RawCopy v1.0.0.15

Writing: $MFT

Job took 7.38 seconds

c:\Users\        \Desktop>
```

```
c:\Users\        \Desktop>FGET.exe -extract c:\$Mft .\$MFT2
-= FGET v1.0 - Forensic Data Acquisition Utility - (c)HBGary, Inc 2010 =-
[+] Extracting File From Volume ...SUCCESS!

c:\Users\        \Desktop>
```

Figure 6-35. RawCopy and FGET

There are several free third-party tools available to collect locked files (including a PowerShell script[222]) which are discussed in various forums by Incident Response analysts[223]. Whatever tool is used- Joachim Schicht' s RawCopy, Greg Hoglund' s FGET, or similar- the files that should be collected for metadata analysis include at least the following:

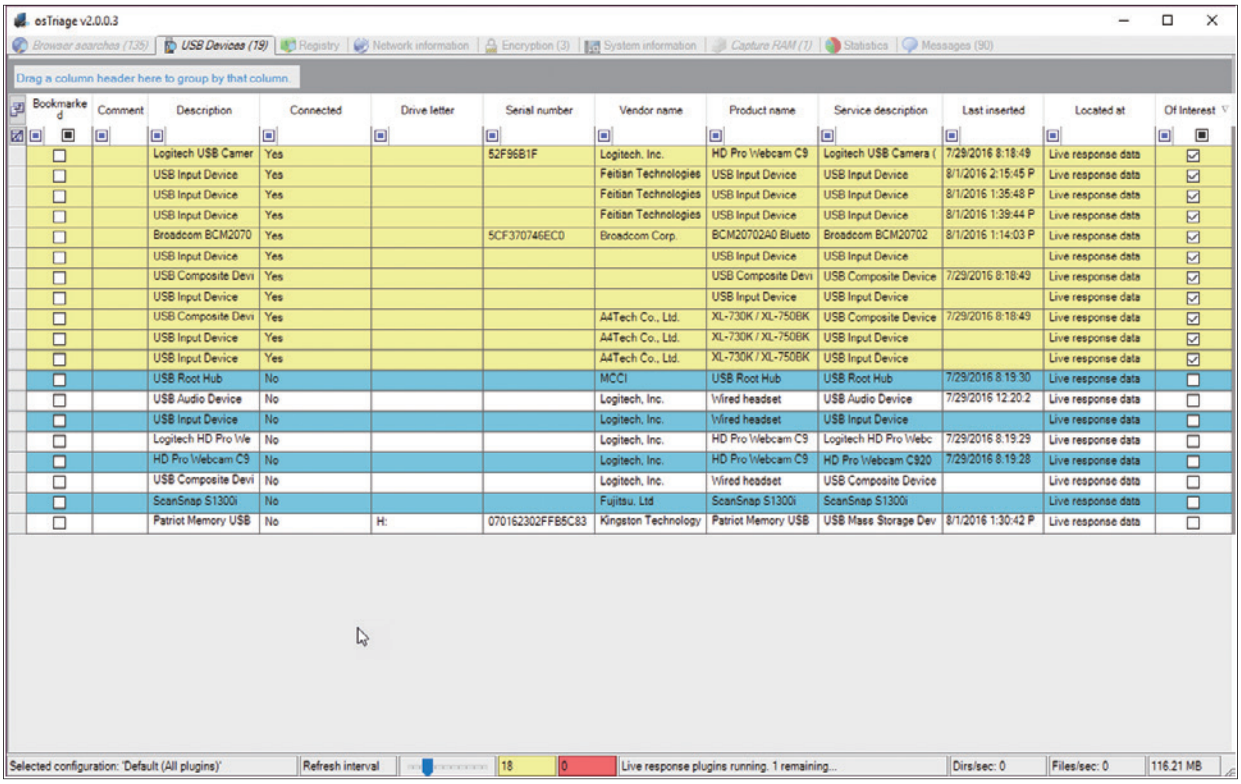
- $MFT and $USNJrnl
- REG hives (System, Software, Security, and SAM)
- User history (NTUser.DAT, USRClass.DAT, and Internet – i.e. Index.DAT, etc.)
- EVT/EVTX logs (Application, Security, and System)
- Antivirus logs
- Volatile system data (TASKLIST, NETSTAT, ARP, IPCONFIG, and Autorun Entries)
- (Optional) Pagefile.sys and Hiberfil.sys
- (Optional) Memory Dump

Fortunately, it is not necessary to collect these artifacts one at a time, as other "Triage" tools have become available from Information Security/Incident Response analysts. The most popular include the

[222] https://github.com/clymb3r/PowerShell/tree/master/Invoke-NinjaCopy
[223] For example, see http://journeyintoir.blogspot.com/2013/09/tools-to-grab-locked-files.html

"Google Rapid Response" (GRR) Framework[224], the "PowerForensics" digital forensics framework[225], "osTriage"[226], and Brimor Labs' "Live Response Collection Toolkit"[227]. Figure 6-36 shows a screenshot of osTriage.

These tools are either installed or may simply need to be called by a suitable command line (i.e., PowerShell as an "Administrator" for PowerForensics or PSRecon as mentioned before).



Bookmarked	Comment	Description	Connected	Drive letter	Serial number	Vendor name	Product name	Service description	Last inserted	Located at	Of Interest
□		Logitech USB Camer	Yes		52F96B1F	Logitech, Inc.	HD Pro Webcam C9	Logitech USB Camera (	7/29/2016 8:18:49	Live response data	☑
□		USB Input Device	Yes			Feitian Technologies	USB Input Device	USB Input Device	8/1/2016 2:15:45 P	Live response data	☑
□		USB Input Device	Yes			Feitian Technologies	USB Input Device	USB Input Device	8/1/2016 1:35:48 P	Live response data	☑
□		USB Input Device	Yes			Feitian Technologies	USB Input Device	USB Input Device	8/1/2016 1:39:44 P	Live response data	☑
□		Broadcom BCM2070	Yes		5CF370746EC0	Broadcom Corp.	BCM20702A0 Blueto	Broadcom BCM20702	8/1/2016 1:14:03 P	Live response data	☑
□		USB Input Device	Yes				USB Input Device	USB Input Device		Live response data	☑
□		USB Composite Devi	Yes				USB Composite Devi	USB Composite Device	7/29/2016 8:18:49	Live response data	☑
□		USB Input Device	Yes				USB Input Device	USB Input Device		Live response data	☑
□		USB Composite Devi	Yes			A4Tech Co., Ltd.	XL-730K / XL-750BK	USB Composite Device	7/29/2016 8:18:49	Live response data	☑
□		USB Input Device	Yes			A4Tech Co., Ltd.	XL-730K / XL-750BK	USB Input Device		Live response data	☑
□		USB Input Device	Yes			A4Tech Co., Ltd.	XL-730K / XL-750BK	USB Input Device		Live response data	☑
□		USB Root Hub	No			MCCI	USB Root Hub	USB Root Hub	7/29/2016 8:19:30	Live response data	□
□		USB Audio Device	No			Logitech, Inc.	Wired headset	USB Audio Device	7/29/2016 12:20:2	Live response data	□
□		USB Input Device	No			Logitech, Inc.	Wired headset	USB Input Device		Live response data	□
□		Logitech HD Pro We	No			Logitech, Inc.	HD Pro Webcam C9	Logitech HD Pro Webc	7/29/2016 8:19:29	Live response data	□
□		HD Pro Webcam C9	No			Logitech, Inc.	HD Pro Webcam C9	HD Pro Webcam C920	7/29/2016 8:19:28	Live response data	□
□		USB Composite Devi	No			Logitech, Inc.	Wired headset	USB Composite Device		Live response data	□
□		ScanSnap S1300i	No			Fujitsu. Ltd	ScanSnap S1300i	ScanSnap S1300i		Live response data	□
□		Patriot Memory USB	No	H:	070162302FFB5C83	Kingston Technology	Patriot Memory USB	USB Mass Storage Dev	8/1/2016 1:30:42 P	Live response data	□

Selected configuration: 'Default (All plugins)' | Refresh interval | 18 | 0 | Live response plugins running. 1 remaining... | Dirs/sec: 0 | Files/sec: 0 | 116.21 MB

Figure 6-36. osTriage

These tools allow investigators to collect volatile data from live computers. They also allow searching across one or more drives for many kinds of files or artifacts. Thorough reports are generated for each search and allow for the validation of results. As mentioned previously, these toolkits combine the built-in utilities found in each operating system, custom scripting, or programming along with other freely available tools. These combined tools support the deeper analysis necessary in the second phase of evidence collection (Investigate) to determine whether the systems of interest include actual evidence of cybercrimes, contain other anomalies such as organizational policy violations, or are irrelevant.

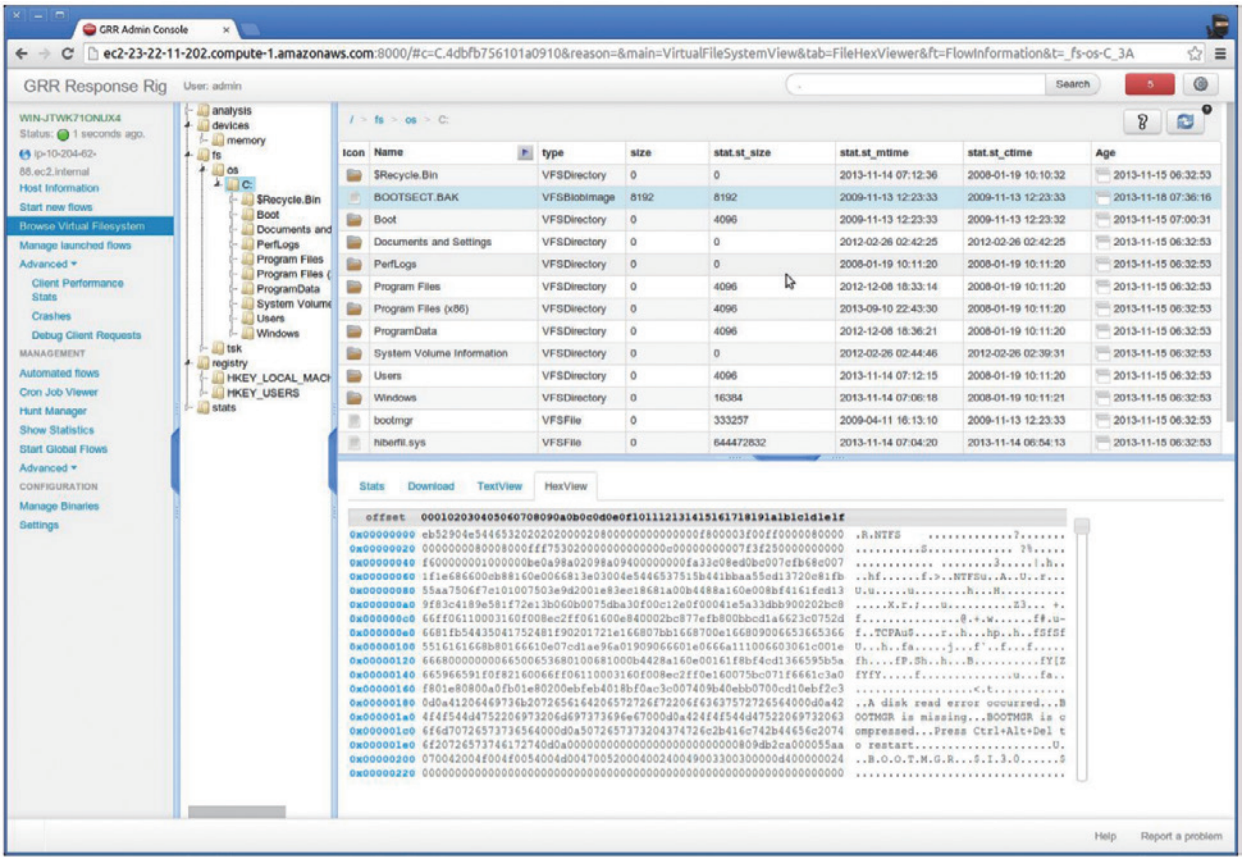
It is important to note that changes will be made on a running system when live collection is performed. This is unavoidable, as an investigator must introduce tools to a running environment and in doing so new artifacts are added to a computer; for example, Registry entries related to a USB device connected to a machine that contains the software which will be used to collect live response data. It is important that the investigator is able to articulate and explain what changes (if any) they

[224] https://github.com/google/grr
[225] https://github.com/Invoke-IR/PowerForensics
[226] https://feeble-industries.com/forums/
[227] https://www.brimorlabs.com/tools/

made to the source evidence due to their actions and to specify the specific tools used. Changes to the source evidence may be unavoidable in a live forensic response scenario, but an investigator' s inability to explain what they were responsible for changing (and why) may result in the evidence being excluded from legal proceedings and may impact the credibility of the investigator' s report or testimony.

●Host Files/Content

The forensic collection of host files or content can be performed with certain manual tools such as FGET or PowerForensics, as discussed. These utilities are intended to assist with acquiring metadata for "lightweight" collections that can be consumed by ETL for efficient processing of results at scale. Other software has traditionally served enterprise forensic collection needs. These tools are fundamentally based upon "Disk Duplicator" (DD). The most popular large scale collection tools include FTK Imager[228], EnCase[229], and X-Ways[230]. Google Rapid Response (GRR) also supports large-scale collection (see Figure 6-37 below), however, and it is important to note that any of these collection tools can collect as much or as little volatile data, disk, and memory contents as is required.



Icon	Name	type	size	stat.st_size	stat.st_mtime	stat.st_ctime	Age
	$Recycle.Bin	VFSDirectory	0	0	2013-11-14 07:12:36	2008-01-19 10:10:32	2013-11-15 06:32:53
	BOOTSECT.BAK	VFSBlobImage	8192	8192	2009-11-13 12:23:33	2009-11-13 12:23:33	2013-11-18 07:36:16
	Boot	VFSDirectory	0	4096	2009-11-13 12:23:33	2009-11-13 12:23:32	2013-11-15 07:00:31
	Documents and Settings	VFSDirectory	0	0	2012-02-26 02:42:25	2012-02-26 02:42:25	2013-11-15 06:32:53
	PerfLogs	VFSDirectory	0	0	2008-01-19 10:11:20	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files	VFSDirectory	0	4096	2012-12-08 18:33:14	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files (x86)	VFSDirectory	0	4096	2013-09-10 22:43:30	2008-01-19 10:11:20	2013-11-15 06:32:53
	ProgramData	VFSDirectory	0	4096	2012-12-08 18:36:21	2008-01-19 10:11:20	2013-11-15 06:32:53
	System Volume Information	VFSDirectory	0	0	2012-02-26 02:44:46	2012-02-26 02:39:31	2013-11-15 06:32:53
	Users	VFSDirectory	0	4096	2013-11-14 07:12:15	2008-01-19 10:11:20	2013-11-15 06:32:53
	Windows	VFSDirectory	0	16384	2013-11-14 07:06:18	2008-01-19 10:11:21	2013-11-15 06:32:53
	bootmgr	VFSFile	0	333257	2009-04-11 16:13:10	2009-11-13 12:23:33	2013-11-15 06:32:53
	hiberfil.sys	VFSFile	0	644472832	2013-11-14 07:04:20	2013-11-14 06:54:13	2013-11-15 06:32:53

```
  offset   000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
0x00000000 eb52904e544653202020200002080000000000000000f800003f00ff0000080000 .R.NTFS    ..............?.......
0x00000020 0000000080008000fff7530200000000000000c00000000007f3f250000000000 ..........S.............. ?%.....
0x00000040 f6000000010000000be0a98a02098a09400000000fa33c08ed0bc007cfb68c007 ............ ........3.....!.h..
0x00000060 1f1e686600cb88160e0066813e03004e5446537515b441bbaa55cd13720c81fb ..hf......f.>..NTFSu..A..U..r...
0x00000080 55aa7506f7c101007503e9d2001e83ec18681a00b4488a160e008bf4161fcd13 U.u.....u........h...H..........
0x000000a0 9f83c4189e581f72e13b060b0075dba30f00c12e0f00041e5a33dbb900202bc8 .....X.r.;...u...........Z3... +.
0x000000c0 66ff06110003160f008ec2ff061600e840002bc877efb800bbcd1a6623c0752d f................@.+.W......f#.u-
0x000000e0 6681fb54435041752481f90201721e166807bb1668700e1668090066536653666 f..TCPAu$....r..h...hp..h..fSfSf
0x00000100 5516161668b80166610e07cd1ae96a01909066601e0666a11100660306 1c001e U...h..fa.....j...f`..f...f.....
0x00000120 666800000000665006536801006810 00b4428a160e00161f8bf4cd1366595b5a fh....fP.Sh..h...B..........fY[Z
0x00000140 665966591f0f82160066ff0611000316 0f008ec2ff0e160075bc071f6661c3a0 fYfY.....f...............u...fa..
0x00000160 f801e80800a0fb01e80200ebfeb4018bf0ac3c007409b40ebb0700cd10ebf2c3 .....................<.t..........
0x00000180 0d0a41206469736b2072656164206572726f72206f636375727265640 00d0a42 ..A disk read error occurred...B
0x000001a0 4f4f544d475220697320 6d697373696e67000d0a424f4f544d4752206973 2063 OOTMGR is missing...BOOTMGR is c
0x000001c0 6f6d7072657373656400 0d0a5072657373204374726c2b416c742b44656c2074 ompressed...Press Ctrl+Alt+Del t
0x000001e0 6f2072657374617274 0d0a000000000000000000000000000809db2ca000055aa o restart.......................U.
0x00000200 07004200 4f004f0054004d00470052000400240049003300300000d400000024 ..B.O.O.T.M.G.R...$.I.3.0......$
0x00000220 0000000000000000000000000000000000000000000000000000000000000000 ................................
```

Figure 6-37. Google Rapid Response

FTK Imager, EnCase acquisition tool, DD, X-Ways, and GRR are all collection utilities and each has similar analytical review tools (See Figure 6-38 below). EnCase and X-Ways are not free, while

[228] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

[229] https://www.guidancesoftware.com/encase-forensic

[230] http://www.x-ways.net/forensics/index-m.html

the other tools are. Investigators should be aware that although there are some differences between each product, the collection files created by each are standardized to court (and industry practices) accepted formats. This means that analysis can be performed using free tools. Some features are more difficult to access or utilize in different review tools, but the collected file formats are standardized so that organizations can achieve the same results from either free or expensive software, depending upon the skills and experience of their investigators and analysts.

Free tools are relied upon extensively by experienced forensic digital investigators and analysts. In particular, GRR, various PowerShell frameworks, and the "SleuthKit" (with its "Autopsy"[231] review tool) are contributed to by a community of skilled analysts dedicated to improving the tools and procedures used to investigate cybercrimes.

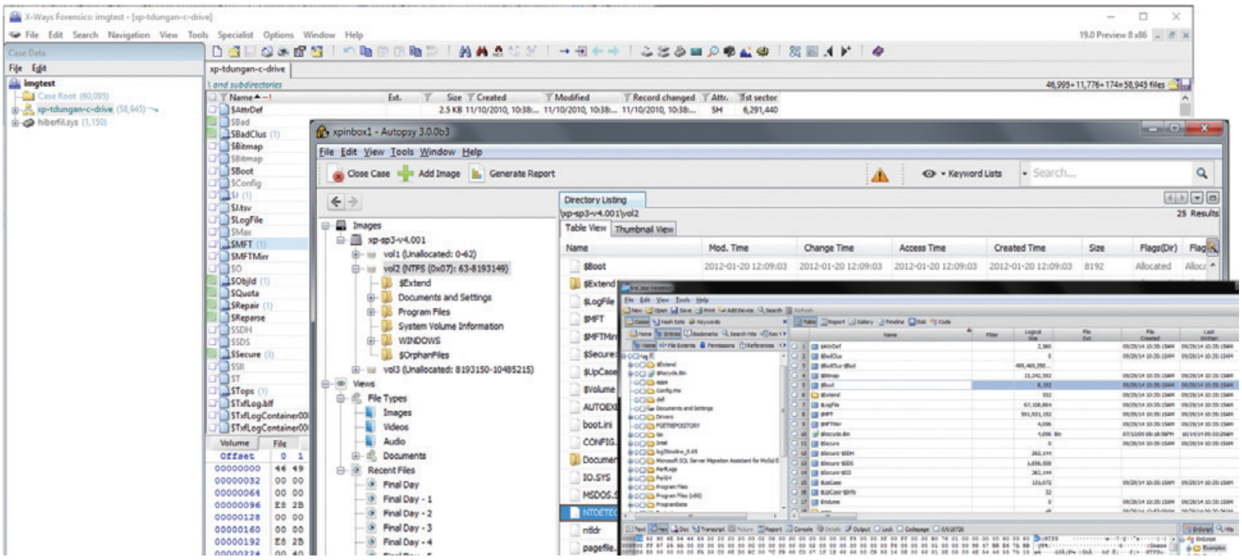


Figure 6-38. Similarities between Forensic Review Tools

The same tools used for digital disk copying can also be used for memory dump collections. Other popular tools are also relied upon for memory collection, including "Fast Dump Professional Edition" (FDPRO)[232] and "Moonsols DumpIt"[233] for Windows, "LiME"[234] for Linux, and "OSXPmem"[235] for Apple/OSX. Once memory is collected, tools such as Volatility and "ReKall"[236] can be utilized to extract information about network connections, running processes, files loaded into memory, operating system and application settings, user history details, and other forensically relevant information.

●Logs

The collection of log files with third-party utilities can be achieved in a variety of ways. Logs can be configured to write their events or to copy their contents periodically to a SIEM system such as Splunk, ArcSight, or similar. Logs can also be remotely accessed and searched and their information can be extracted (or log files can be copied entirely), all through the use of the same

[231] http://www.sleuthkit.org/autopsy
[232] http://www.countertack.com/products
[233] http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7
[234] http://code.google.com/p/lime-forensics/
[235] http://www.rekall-forensic.com/docs/Tools/
[236] http://www.rekall-forensic.com/

toolkits mentioned in the previous section. Like with evidence collection software, log collection and correlation software is available for free or at cost. The essential differences are the requisite skills to engineer, program, deploy, and support the solutions.

Currently, the two most popular log collection and consolidation (for processing) solutions are: an open-source solution from "Elastic" called the "Elastic Stack" (formerly known as "ELK", for Elastic search, Logstash, and Kibana, but now with "Beats" included)[237] that is free to use, except for necessary storage and processing equipment which must be sourced independently; and "Splunk"[238], a solution that is free in some (limited) conditions but is essentially licensed at cost for volume of data processed, which can be expensive. Splunk has a large community of developers (open and proprietary sources) with many tailored solutions and support available in the communities.

As mentioned earlier, both log files and their configuration files should be collected to review for evidence. It is important to understand what information is available from logging sources as well as what information is not, either because of configuration deficiencies or due to technical (often sabotage) reasons.

Logs should be collected for analysis from the following sources to determine potential evidence of cybercrimes:

- Endpoint computers and servers/services (AD/DNS/Proxy, etc.)
- Network switches, bridges, routers, and firewalls
- Phone systems, alarm systems, and access control systems
- Other IT and OT systems (building management, ICS, DCS, etc.)

Logs should be collected, consolidated, tested for quality and relevance, and processed in a correlation system to support procedures for analysis of evidence. Figure 6-39 below details the scope of logging and log management:

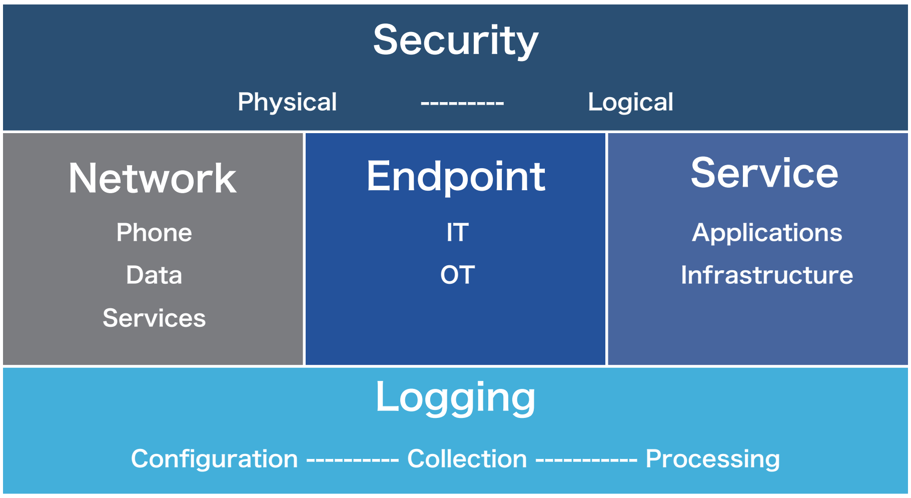

Security
Physical --------- Logical
Network
Phone
Data
Services
Endpoint
IT
OT
Service
Applications
Infrastructure
Logging
Configuration ---------- Collection ----------- Processing

Figure 6-39. Logging

[237] https://www.elastic.co/products

[238] http://www.splunk.com/

Forensic Integrity of Evidence

Methods used to collect evidence should be repeatable, demonstrable, and verifiable. If given the same input(s), the same output(s) can be reliably produced regardless of how many times the process is performed and who performs the actions – the process is repeatable. If the tools and methods used can be reviewed by others to understand how results or conclusions are reached – the process is demonstrable. If different tools or methods can be applied to the same input with reliable procedures and produce the same output – the process is verifiable. These are very important considerations when developing methods and designing or selecting associated tools and staff to collect forensically sound evidence.

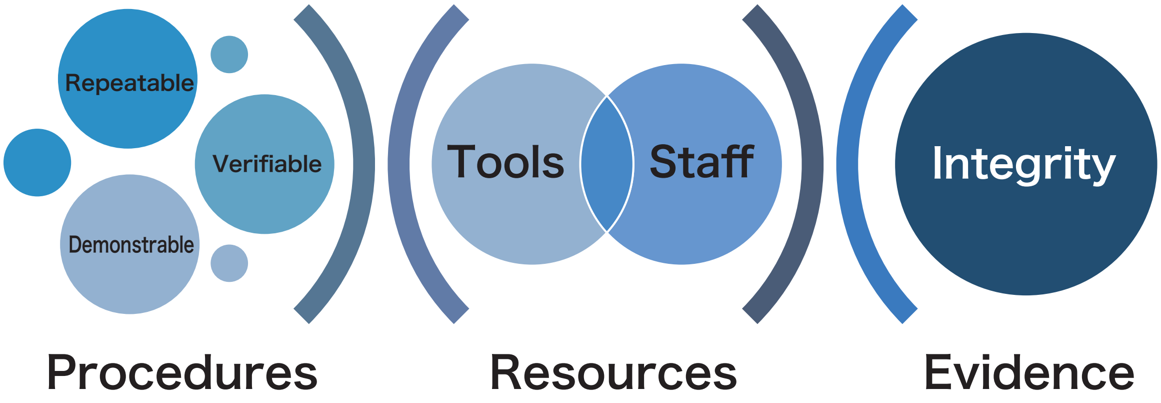


Figure 6-40. Forensic Integrity

The term "forensic" refers to scientific tests or techniques used in the detection of crime. Traditional crime investigations involve evidence collection and expertise from fields such as forensic psychology, pathology, mechanical, ballistics, and accounting. Cybercrimes have introduced the need for cyber forensic expertise.

Cybercrime investigations are not the same type of activities that IT or even information security staff generally perform "in the normal course of business" (a common term used in evidence/witness qualification examinations in legal proceedings). Cybercrime investigations depend upon forensic procedures that guarantee integrity. Integrity is a combination of the voracity of witnesses (staff and experts), the reliability of evidence collection procedures, and the ability to prove both.

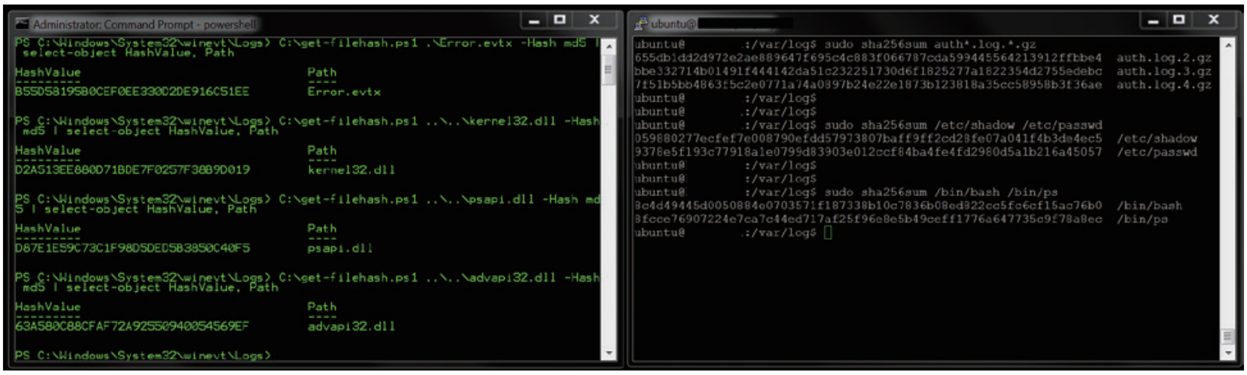
With regard to technical (digital) forensic evidence, a "black box" approach is not sufficient in cyber investigations, although it is used extensively in IT and information security processes that support an organization' s needs. "Proof" is the standard that must be met, and can only be achieved with integrity.

A process that is demonstrable should provide some visibility into how a tool is producing its output so that, if required, an examiner can explain how a conclusion was reached. In other words, examiners should avoid relying on a purely "black box" approach and instead should be able to explain and demonstrate the techniques for collection and transformation of evidence, and how those techniques allowed them to reach a conclusion.

Examples include the use of cryptographic hashing of files or an image of a hard drive, or verifying one forensic tool with another or against a documented specification.

Cryptographic hashing[239] functions are essentially a method of computing a mathematical “checksum” that takes a stream of data, such as a file input, into a programmed algorithm and returns a fixed value as a “hash signature”. The signature is unique, as any change in the subject file will cause a change in the value returned from the algorithm through subsequent tests. In other words, a hash function is any algorithm that maps variable length data (such as contents of a file) to fixed length data (size). Hash signatures are widely used as reliable evidence that files have not been tampered with during evidence collection, and that the same files that one examiner/expert relies upon for their conclusions are available for examination by another.

The hash signature should not be confused with a cryptographic message signature. Hashing a file does not relate in any way to encrypting a file- it is merely a unique signature that represents the file (as opposed to file names that are often redundant). The most utilized hash functions for verifying collected evidence are MD5 and SHA256. Windows and Linux have built-in capabilities to compute hashes by utilizing scripts[240] (see Figure 6-41) but many other tools are also available with these capabilities, including the previously mentioned collection tools. The inability to prove the integrity of collected evidence can impede a cybercrime investigation, so the capability to compute hashes-regardless of the tool used- is critical.



```
PS C:\Windows\System32\winevt\Logs> C:\get-filehash.ps1 .\Error.evtx -Hash md5 |
 select-object HashValue, Path

HashValue                                 Path
---------                                 ----
B55D58195B0CEF0EE330D2DE916C51EE          Error.evtx

PS C:\Windows\System32\winevt\Logs> C:\get-filehash.ps1 ..\..\kernel32.dll -Hash
 md5 | select-object HashValue, Path

HashValue                                 Path
---------                                 ----
D2A513EE880D71BDE7F0257F3889D019          kernel32.dll

PS C:\Windows\System32\winevt\Logs> C:\get-filehash.ps1 ..\..\psapi.dll -Hash md
5 | select-object HashValue, Path

HashValue                                 Path
---------                                 ----
D87E1E59C73C1F98D5DED5B3850C40F5          psapi.dll

PS C:\Windows\System32\winevt\Logs> C:\get-filehash.ps1 ..\..\advapi32.dll -Hash
 md5 | select-object HashValue, Path

HashValue                                 Path
---------                                 ----
63A580C88CFAF72A92550940054569EF          advapi32.dll

PS C:\Windows\System32\winevt\Logs>
```

```
ubuntu@         :/var/log$ sudo sha256sum auth*.log.*.gz
655db1dd2d972e2ae889647f695c4c883f066787cda599445564213912ffbbe4  auth.log.2.gz
bbe332714b01491f444142da51c232251730d6f1825277a1822354d2755edebc  auth.log.3.gz
7f51b5bb4863f5c2e0771a74a0897b24e22e1873b123818a35cc58958b3f36ae  auth.log.4.gz
ubuntu@         :/var/log$
ubuntu@         :/var/log$
ubuntu@         :/var/log$ sudo sha256sum /etc/shadow /etc/passwd
059880277ecfef7e008790efdd57973807baff9ff2cd28fe07a041f4b3de4ec5  /etc/shadow
9378e5f193c77918a1e0799d83903e012ccf84ba4fe4fd2980d5a1b216a45057  /etc/passwd
ubuntu@         :/var/log$
ubuntu@         :/var/log$
ubuntu@         :/var/log$ sudo sha256sum /bin/bash /bin/ps
8c4d49445d0050884e0703571f187338b10c7836b08ed822cc5fc6cf15ac76b0  /bin/bash
8fcce76907224e7ca7c44ed717af25f96e8e5b49ceff1776a647735c9f78a8ec  /bin/ps
ubuntu@         :/var/log$ 
```

Figure 6-41. Windows and Linux Native Hashing

Procedure Documentation

Evidence collection requires very specific documentation. In part, documentation helps to ensure the forensic integrity of evidence, but it is also essential because evidence collection is part of a process that supports an overall investigation of a crime. A documented forensic procedure that meets all the identified requirements (repeatable, demonstrable, and verifiable) can be followed by any examiner to produce consistent results. However, this is not to suggest that a documented process relieves the investigator of understanding what they are doing. Part of the documentation should include the name and relevant qualifications of the investigator who collects the evidence, as well as any staff who assist or handle the evidence from its collection until its eventual destruction or handover to other authorities.

[239] http://www.forensicswiki.org/wiki/Hashing

[240] Windows PowerShell 5.0 has Get-Filehash CMDLET built-in but older versions of PowerShell will need a suitable script such as http://poshcode.org/5815; similar scripting can be performed with Visual Basic Scripting (and using .NET) such as demonstrated at http://mwganson.freeyellow.com/md5/md5.vbs

Documentation can include an overview of why a particular source or given artifact is valuable, how it is generally interpreted, and other relevant context. This enables better report generation and trial or legal procedure preparation, as the specifics surrounding the collection of evidence can assist other parties in the resolution or prosecution that may follow a cybercrime investigation.

Documentation of procedures for collecting evidence should contain at least the following:

- Sources of available evidence – including intelligence, personnel, and systems
- Methods of collection – including staff (internal and third-party support), tools, and processes
- Collection and handling policies – including legal, risk management, and communications guidance

Documented procedures also support continuity of operations as personnel rotate in and out of an organization. By having thorough documentation of collection procedures, the learning curve for people unfamiliar with an organization' s process can be greatly reduced.

Tools Certification(s)

Tools used for the forensic collection of evidence should be certified. The certification can be simply administered through documented procedures that are periodically audited and updated by qualified internal staff or third parties. Documentation can also be supported by product information provided by vendors with regard to when and how a product has been used in similar circumstances; however, the specific use or conditions of use of tools are always questioned in legal proceedings. Therefore, tools used for evidence collection should be utilized in accordance with organizational procedures, or at least by staff who are capable of specifically detailing the methods of the tools' use in the process of evidence collection.

It is important to note that courts do not certify forensic tools. Rather, the process an examiner used (along with their reasons for following those procedures) are scrutinized by the courts and serve to determine whether the data being introduced in a trial is admissible. Court proceedings are where the previously discussed items all come together. If an investigator follows a defined process and understands the sources and methods of collection, they will be able to articulate everything to the court and satisfy the requirements to be deemed a credible and reliable witness - or in some cases, an expert witness.

Tool certification by a third-party can often serve as a starting point for an organization' s selection of a given tool; however, it should never replace internal testing and verification by qualified investigators. Another aspect of certifications is that of investigators becoming certified in the use of a specific tool. This can range from taking an online test to a comprehensive demonstration, not only of proficiency with the tool but, more importantly, with forensic concepts and techniques. Investigators should strive to use tools and not be "used by" tools. In other words, tools are only as useful as the people who use them. If they are used incorrectly or if the investigator does not understand why and when they should be used (or not), tools will not be suitably reliable to their requirements. Forensic tools and industry certifications often can serve to show mastery of a particular product or standard method. However, a certification should not be solely relied upon to determine an investigator' s competency in evidence collection.

Acquirer and Analyst Qualification(s)

There are many certifications that IT or related technical staff can pursue during their career. Some require secondary education (college degrees) but most are industry or vendor certifications intended to demonstrate mastery of a subject or technology; however, many investigators do not possess certification[241]. Instead, their experience, practices, methods, and knowledge provide the value that many who have been certified still need time and opportunity to develop.

There are a wide variety of industry certifications that are vendor-neutral such as SANS FOR 408 (Windows Forensic Analyst[242]), SANS FOR 508 (Advanced Digital Forensics and Incident Response[243]), and SANS FOR 572 (Advanced Network Forensics and Analysis[244]). These courses present a wealth of material and each culminates in an associated test and a certification. The two most common vendor certifications are AccessData Certified Examiner (ACE) and EnCase Certified Examiner (EnCE), though the following vendor-neutral certifications are also common throughout the industry:

- **CCE** – International Society of Forensic Computer Examiners/Certified Computer Examiner
- **CHFI** – International Council of E-Commerce Consultants/Computer Hacking Forensic Investigator
- **CFCE** – International Association of Computer Investigative Specialists/Certified Computer Forensic Examiner
- **GCFE** – Global Information Assurance Certification/Certified Forensic Examiner
- **GCFA** - Global Information Assurance Certification/Certified Forensic Analyst
- **CSFA** – CyberSecurity Institute/Cyber Security Forensic Analyst

Staff who perform evidence collection should be detail-oriented, succinct writers, and possess the ability to explain complex technical concepts to varying audiences. For example, presenting findings to other investigators and examiners will include more (and different) details than when presenting findings to a lawyer or executives who may not have the same technical background.

Requirements by Type of Cybercrime

Collection requirements differ, as evidence requirements vary according to the type of cybercrime. The type of cybercrime is defined by the target (and corresponding scope) as well as by the category(the intent or objective of the crime). The targets and categories of cybercrime have direct parallels to traditional crimes. The types of evidence to be collected often result from what a prosecutor will need to use to prove a case in court. Evidence collection an organization or investigator is tasked with should be prioritized by the target and category of criminal intent. Any case that involves the safety of a person will take a higher priority than one that does not. For example, an imminent terrorist threat or kidnapping will take a higher priority than financial fraud or

[241] http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications
[242] https://www.sans.org/course/windows-forensic-analysis
[243] https://www.sans.org/course/advanced-incident-response-threat-hunting-training
[244] https://www.sans.org/course/advanced-network-forensics-analysis

intellectual property theft.

The following sections will discuss the types of evidence to collect as well as priorities to consider when investigating each target and category of cybercrime. Where useful, examples of evidence to collect are presented as well.

By Target

As mentioned in earlier chapters, cybercrimes reflect new mechanisms for committing crime. For evidence collection purposes (of intelligence sources and investigative artifacts), the types of cybercrimes can be contextualized according to the target of the crime. Certain evidence is common to all cybercrimes and necessary for collection, processing, and analysis; however, prosecutors may request focused assessment and additional specific collection(s) of some sources of evidence and related artifacts.

●Person

Cybercrimes that target individuals leverage personally identifiable information (PII). As such, the person' s history of use with computers and mobile devices serves as the best source of evidence. Beyond the common artifacts such as the $MFT or change logs for the filesystem, NTUSER.DAT (or .bash_history and related files), PLists, email stores (such as PST and OST files), and internet browser histories should be processed for timeline analysis and examined for IOCs that correlate with intelligence sources.

●Organization

Cybercrimes that target an organization have objectives that may not be as simple as those targeted at an individual. The nature and scope of the targeting is only determinable with a comprehensive analysis of intelligence and investigative evidence sources including host and network data. Emphasis in analysis should be placed on discerning which (if any) organizational unit(s) have been targeted and for what purposes. For example, if intelligence sources indicate a company has been targeted for intellectual property theft, the examination should focus on the development and storage of related IP versus financial or human resources applications. Procedural investigative steps (such as those previously described) will still reveal other Systems of Interest; however, prioritizing collection and analysis according to the objective targeting will ensure efficient resource utilization.

●Industry

Similar to the targeting of an organization, the targeting of an industry segment should involve collection of evidence related to the objectives of the cybercrime. A particular emphasis on intelligence collection from OSINT and PROPINT, including peer organizations and industry community information sources, is paramount to create and utilize IOCs with security automation tools (for alerting and other purposes).

●Nation

Targeting of nation-states is typically directed against defense or political information, communications, and operations networks and management systems. The intent of such activities is primarily to conduct espionage, subversion (through reconfiguration or misinformation), or sabotage/

destruction. Evidence collection in such cases should focus on intelligence data that can detail specific industries, organizations, or persons, and associated technical indicators that can assist investigators with forensic evidence acquisition.

By Category

Cybercrimes are committed to achieve certain objectives according to the scale of their target(s). The following table includes some categories that organizations and cyber investigators should incorporate into collection guidance policies and procedures:

Table 6-1. Evidence Collection by Category

Category	Objective	Sources of Evidence
Health and Human Safety	Healthcare or Emergency Response Services	• Video/Audio and safety systems recordings/logs • Phone call logs/recordings • Interviews with witnesses • User endpoint and application services (Email/Chat/etc.) images • User network shares
	Violence against Persons	
	Child Crimes	
	Kidnapping	
	Identity Theft	
	Destruction of Property or Facilities	
Extortion/Theft	Blackmail	• Phone call logs/recordings • Interviews with witnesses • Endpoint/Server and application services (Email/Chat/etc.) images • Market intelligence and OSINT/PROPINT
	Personal Finances	
	Organizational Finances	
	Industry Financials/Economic Performance	
	Market Financial/ Performance	
Commercial	Software Intellectual Property	• Phone call logs/recordings • Interviews with witnesses • Endpoint/Server images
	Other Intellectual Property (Designs, Blueprints, etc.)	
Terrorism and National Security	Sabotage/Subverions/Fear	• All of the above (as required)

● Handling of Evidence

Evidence should always be handled with the understanding that it may be used in a trial setting. As such, it is vital to properly document all stages of evidence handling, from initial collection through the examination process and returning said evidence to its owner. Legal restrictions should guide policies concerning collection methods regarding privacy, sensitivity of information, and access controls.

Collection Guidance

There are three types of evidence that will be collected when dealing with cybercrime: incidental evidence collected upon detection or suspicion of a cybercrime (through standard organizational processes), evidence collected on-scene as a result of a physical search warrant or similar action, and evidence collected via subpoena, electronic search warrant, or other legal process.

In the case of a physical search warrant, it often takes days or weeks to first secure the proper legal paperwork and submit it to an internet service provider, then for the provider to gather evidence and return it to the requesting agency. In any case with such circumstances, it is recommended that a preservation request is sent to the entities who hold or control the evidence that will be requested (when proper legal authority has been granted). The preservation request should make it clear that the owner of the information being sought is not to be informed of the request (according to jurisdictional requirements). If the company that holds the evidence tells the owner of the information about the request, the investigation could be jeopardized; for example, the subject could then attempt to modify or destroy the evidence.

●Incidental evidence collection

Incidental evidence collection is essentially the "normal course of business" collection of intelligence and evidence that occurs with organizational processes and related technology. There should not be additional evidence collection performed as such unless organizational policies describe exceptions. Such exceptions might include help desk, IT, audit, security, or related procedures to escalate suspicious activities to investigative actions, in order to collect and preserve evidence related to anomalies detected during the normal course of business. Such escalation procedures should be incorporated into organizational risk management policies to ensure that other business activities do not impede subsequent evidence collection or diminish the reliability of evidence due to accidental tampering. This is an unfortunate but very common situation that investigators are faced with when help desk or IT staff attempt to "help" but do not understand requirements (purpose and restrictions) concerning the methods of evidence collection.

●Physical evidence collection

The collection of digital evidence is similar in many ways to more traditional evidence collection for blood, paper records, or weapons- the location of the evidence and the environmental conditions in which it was found sometimes matter as much as (or more than) the contents of the evidence itself.

As a matter of policy, upon securing a location investigators should - take a video of the scene to document the environment before conducting a search. While photographs can also be used, video is often quicker and enables greater preservation of detail, as it provides more information that (when compared with photographs) investigators can more efficiently collect. After the "before" state is recorded, specific areas in the location should be given a designation such as a unique letter or number. A sketch of the overall location can also be made, and the designators can be recorded on the sketch for ease of reference later in the investigation.

Once the search is underway, investigators should thoroughly document their findings as evidence is located. This includes recording the area where evidence is found, its location within the area, and who found the evidence. Before collecting digital evidence, the state of the digital device should be observed. Some examples include but are not limited to whether the device is powered on, what the device is connected to, and so on. To summarize, prior to collecting digital evidence, a photograph of the device should be taken and the following specific information should be documented:

- Who found the item
- What date/time was it found

- What area and location it was found in
- The state of the device (powered on, plugged in, etc.)
- Make, model, serial #, and other identifying details of the device

As each piece of evidence is found, it should be taken to a custodian. Each item should be placed in its own plastic bag and given a unique number, which is written both on the bag and on the inventory of what is being seized. If the device to be collected is powered on, it is often advantageous to collect any available volatile data from the device, such as what is visible on the screen, running processes, and so on. Photographs of the screen and detailed notes of what is visible should be taken if the photographs do not clearly show what is present on the screen. Once the initial state of the device is recorded, the device should be triaged to gather volatile data that would be lost if the device were powered down. Tools such as osTriage, PSRecon, or other live response tools (as previously mentioned) allow investigators to quickly gather both volatile and non-volatile data and present it in a convenient format which they can use to make immediate decisions about what to do next with a given device.

Triaging devices will automate many critical evidence collection techniques, such as determining if the device is encrypted. This is vital because strong encryption is becoming more and more common, and if such devices are not handled properly the ability to access data later will be more difficult or sometimes impossible if the device is powered off prematurely. Triaging can also provide a wealth of real-time intelligence that can be used on-scene during interviews with suspects and witnesses. For example, the triage data might indicate connections with other hosts in the network (or other locations) that may yield useful evidence upon subsequent collection and analysis. The triage process can provide a list of browsing history, recent files and programs used, and so on. That information can also be integrated into interviews for additional evidence.

At the conclusion of the search, the inventory should be reviewed with the person who owns the property so they can review what is being collected. Once the review is completed, the person who prepared the inventory and the owner of the items being seized should sign the inventory receipt. A copy of the inventory should be provided to the person who signs the inventory. A copy of the paperwork authorizing the search warrant (minus any statement of facts) should be provided as well. It is also recommended that a photograph is taken of the inventory receipt and the search warrant to show that a service copy was provided. Ideally, investigators should take a photograph of the person who signed the inventory holding both the inventory and the service copy of the search warrant. This removes the possibility of any claim that they were not provided with copies of those documents.

●Electronic evidence collection

This category of evidence results in an organization being served with a legal process such as a subpoena or search warrant. Electronic materials could be as simple as an email account, a server or end user computer, an application history log and correlated configuration file(s), or computer/memory images and network packet captures. The type and format of information returned through electronic evidence collection can vary greatly depending on the subject of the subpoena and how they have decided to return the requested materials– or how investigators seize, collect, and document evidence pursuant to the search warrant. Regardless of what is returned, it should be handled in a consistent manner. The following information should be recorded in a report, evidence tracking system, or similar repository upon receipt from the provider:

- The date and time of the evidence delivery
- A reference to the legal process that prompted the provider to gather data
- A summary of the materials delivered, including a picture and detailed inventory
- The identity and address of the provider of the evidence, including the delivery person or agent

A working copy should be made of electronic evidence, for analysts to work from. It is never advisable to work with original evidence once it is collected unless making a copy of the evidence for investigative purposes. Special procedures to copy the evidence and protect the forensic integrity of the evidence should be used such as a "write blocker" that prevents modification of file system or volume data, or in lieu of that, specific documentation (sometimes accompanied by a video of copy procedures). Hash signatures of the original evidence and each copy made should be documented as well, to verify the integrity of the evidence.

Even if law enforcement is not involved in cybercrime investigations, it is best practice to follow these procedures in organizational security and investigations activities. Documenting these procedures in relevant policies can also assist risk management, IT, and associated groups with understanding the requirements to support law enforcement requests in cybercrime evidence collection.

Challenges in Evidence Collection

The proliferation of embedded devices presents unique challenges to modern evidence collection. The methods and tools presented in this chapter represent a comprehensive approach for traditional endpoints where a user has easy access to the device and where the system architecture and operating system architecture supports common applications. However, the rise of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices often require additional sophisticated extraction and analysis tools.

Internet of Things (IoT) Devices

By default, IOT devices often contain a stripped down kernel and offer limited access to the device file system. As a result, they frequently rely on cloud services and websites for management. However, many IoT vendors build hardware debugging ports or limited local interfaces where data collection may be possible.

IoT devices run a variety of operating systems, from Android to other Linux variants. Even with access to IoT devices, the evidence generated may vary greatly from device to device due to configurations, space limitations, and the features developers have left running on the specific device. On IoT and embedded devices, it is common to see a stripped down software suite called "BusyBox" with a limited number of command line commands present. Evidence collection on IoT devices often depends upon knowing what data can be extracted with the commands present on the device' s BusyBox instance, as not all devices ship with the same commands enabled. For devices with exposed web interfaces, investigators can often pull web server artifacts from NGINX or other web servers running on the devices.

Industrial Control System and Industrial Internet of Things (IoT) Devices

Industrial Control System (ICS) devices and Industrial Internet of Things (IIoT) devices are a subclass of IoT devices designed to run in industrial environments. Industrial devices in these categories include sensors, actuators, human machine interface devices, and other endpoint devices.

Sensors monitor the state of the industrial process both to ensure it performs as intended and, in the case of a safety system, to quickly react and alert the overall system that an adjustment needs to be made to protect the integrity, availability, and safety of the process.

Actuators act in the physical world and cause some form of physical change. Examples include a robot, a motor, and any other device capable of physical or process control changes.

Human machine interfaces include devices that plant operators or other personnel use to monitor and control the industrial process.

Evidence collection may or may not be straightforward with industrial devices. For instance, human machine interfaces often use different versions of Microsoft Windows. If Windows is installed on a traditional endpoint system, an investigator may be able to collect traditional Windows artifacts directly from the system; however, challenges may arise with vendor managed systems requiring coordination with the vendor for access, such as when human machine interface devices are on embedded systems For example, Siemens produces the Simatic HMI series which ships Windows CE on an embedded system. In this case, it may not be as straightforward to collect evidence from this endpoint, and the investigator might have to determine what log and data sources are accessible.

Programmable logic controllers (PLCs) present an even greater challenge for evidence collection. Many of these devices run real time operating system (RTOS) variants such as Blackberry' s QNX or WindRiver' s VxWorks. In these situations, both access methods and artifacts will be very different than those of Windows endpoints. Collection from a PLC or embedded device may require a certain amount of hardware reverse engineering skills, including knowledge of how to access debug ports on the device (if present). Some devices ship with exposed Joint Test Action Group (JTAG) ports, where data or access to an embedded device may be possible. In other cases, working with the manufacturer may be required to collect data. It may also be possible to collect data from an embedded industrial device through software probing. For example, Microsoft has developed an open source tool called ICSpector for probing certain information from ICS systems[245].

Chain of Custody Maintenance

After evidence is seized, it should be securely transported to a designated evidence facility for secure storage. In law enforcement proceedings, this activity will be at the discretion of the agents collecting the evidence according to their procedures. In organizational investigations, evidence facilities should also be designated for use and should have related policies governing physical/logical access controls, as well as related recordings of who deposits evidence and their activities in relation to the original evidence handling. When an evidence facility is not available, due diligence should be exercised by the person in possession of the seized evidence to ensure it remains secure and in the custody of the individual who signed the inventory/receipt. Each seized item should have a chain of custody prepared as previously described.

Once the evidence is delivered (or checked out in electronic evidence case management systems),

[245] https://github.com/microsoft/ics-forensics-tools

the recipient should sign a “control log” detailing how the evidence has been accessed, by whom, when, and why. An example is provided below in Figure 6-42:

Figure 6-42. Chain of Custody Log

Name	Reason	Date/time	Name	Location	Date/time
Steve Allen	Transport from location	2016-08-27 13:47	Mike Rogers ID#1234	Evidence Locker	2016-08-27 15:00
Mike Rogers	Checked out for review	2016-08-28 08:27	Steve Allen ID#6789	Desk	2016-08-28 08:27
Steve Allen	Return to evidence	2016-08-30 09:52	Mike Rogers ID#1234	Evidence Locker	2016-08-30 09:52

Copies of evidence are tracked like any other piece of evidence,and a chain of custody is used accordingly.

Retention by Category/Jurisdiction

Until the case is resolved, evidence- both original and any copies (sometimes called “derivative evidence”)- should be kept and a related chain of custody should be maintained. The timeline for case resolution can range from months to years depending on what happens as a result of a trial. Preparation and planning must be undertaken to ensure adequate storage and resources to maintain dozens or hundreds of cases worth of evidence as cases move through the judicial process (including appeals or reviews as required). Besides legal retention, regulatory requirements may define the retention of certain evidence if it contains personal health, privacy, financial, protected industry, classified, or similar information. Because of these issues, organizations should take particular care when determining policies and procedures for collecting incidental evidence such as SIEM or other logging and audit data. In some instances, the collection of non-public information may incur retention and handling requirements (such as disclosure, in some regions of the world).

Destruction of Evidence

In most cases, at the conclusion of a case the original evidence is returned to its owner. This process should be documented on an inventory sheet in a similar fashion to when the evidence was seized. When the evidence is returned to someone, the inventory is signed by the law enforcement officer returning it as well as the person taking possession of the evidence. This inventory should then be placed in the case file, showing the evidence was returned. If evidence cannot be returned to the owner, any materials should be destroyed with appropriate means, and the destruction should be documented accordingly.

Chapter 6: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts) and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

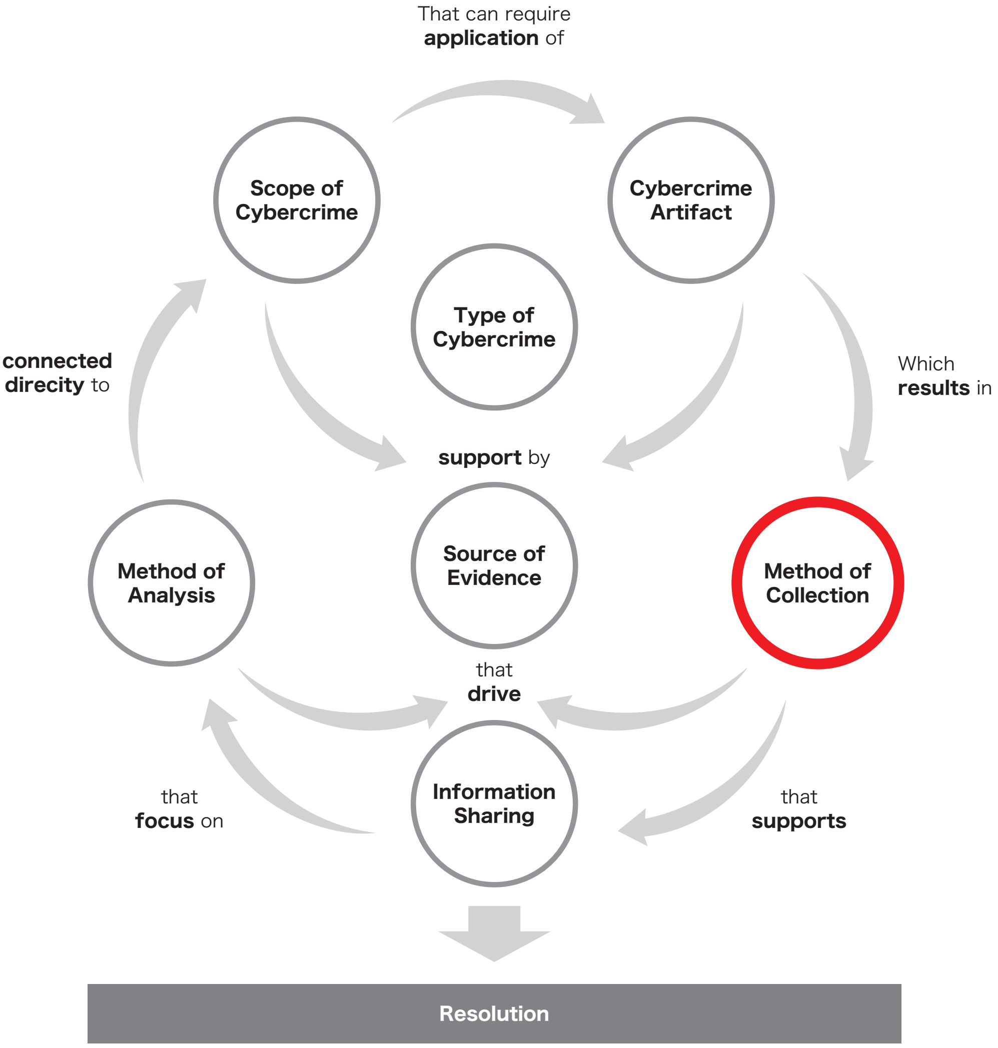


Figure 6-43. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 6-44. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 6-45. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a procedural understanding of jurisdictional guidance concerning evidence collection and handling methods. They should have strategic responsibility for defining and managing related policies.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. Intelligence staff should have a procedural understanding of evidence collection methods (and limitations), and tactical knowledge of how to collect evidence.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigative staff should have a procedural understanding of evidence collection methods (and limitations), and tactical knowledge of how to collect evidence.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well as methods and restrictions concerning collection of evidence to inform policy makers.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The type of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 6: Review

1. How can evidence of cybercrime be collected?

   Answer: Automatically and Manually

   Examples: By intelligence, investigations, and interviews

2. How should evidence of cybercrime be collected?

   Answer: Systemically (alerts-driven), sweep discovery, native and third-party tools

   Examples: SIEM, network PCAP, phase 1/2/3 collections

3. What measures or steps should be taken to ensure reliability of evidence?

   Answer: Plan/Document/Use Procedures, Resources, and Evidence

   Examples: Repeatable/verifiable/demonstrable, staff/tools, integrity

4. How do evidence and related methods of collection differ by type of cybercrime?

   Answer: By Target and By Category

   Examples: According to scope and objectives

Case Study 6: Evidence Collection in Complex IT/OT Environments

- **Crime**: Identity (credential) theft, unauthorized access
- **Suspect(s)**: Nation-state threat actor
- **Means**: Social engineering (spear phishing), hardware and software reverse engineering, malware
- **Motive**: Espionage, disruption of critical infrastructure operations, potential intent to cause physical damage and harm (by disrupting safety systems)

Operations Technology environments that support utilities as well as large-scale water, oil & gas, and other chemical refinement processes are a doubly dangerous situation in a cyber incident. Not only the possibility of interruption of technical systems is at stake, but also safety systems - and human lives. Notorious events related to the use of "Triton/Trisis" malware in a Saudi Arabian petrochemical refinery were discovered in 2017, but only after several months of its use, and as was later learned - actual years after entry by threat actors had initially gained access (in 2014)[246].

Safety systems within an industrial environment continuously monitor, alert, and often react to potentially unsafe situations within industrial environments to protect loss of life, ensure integrity of the industrial process, and optimize production within industrial processes.

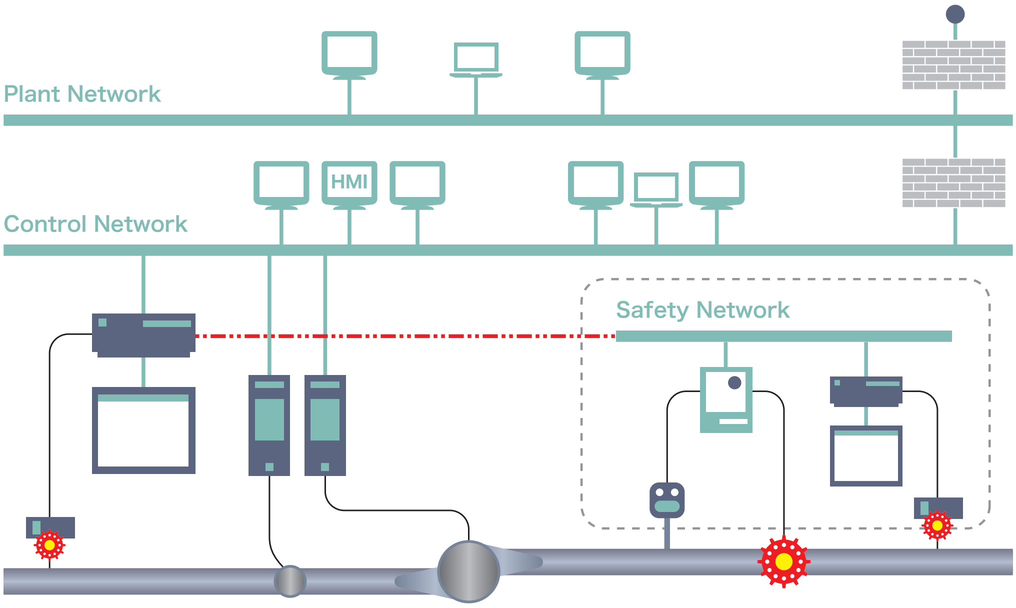
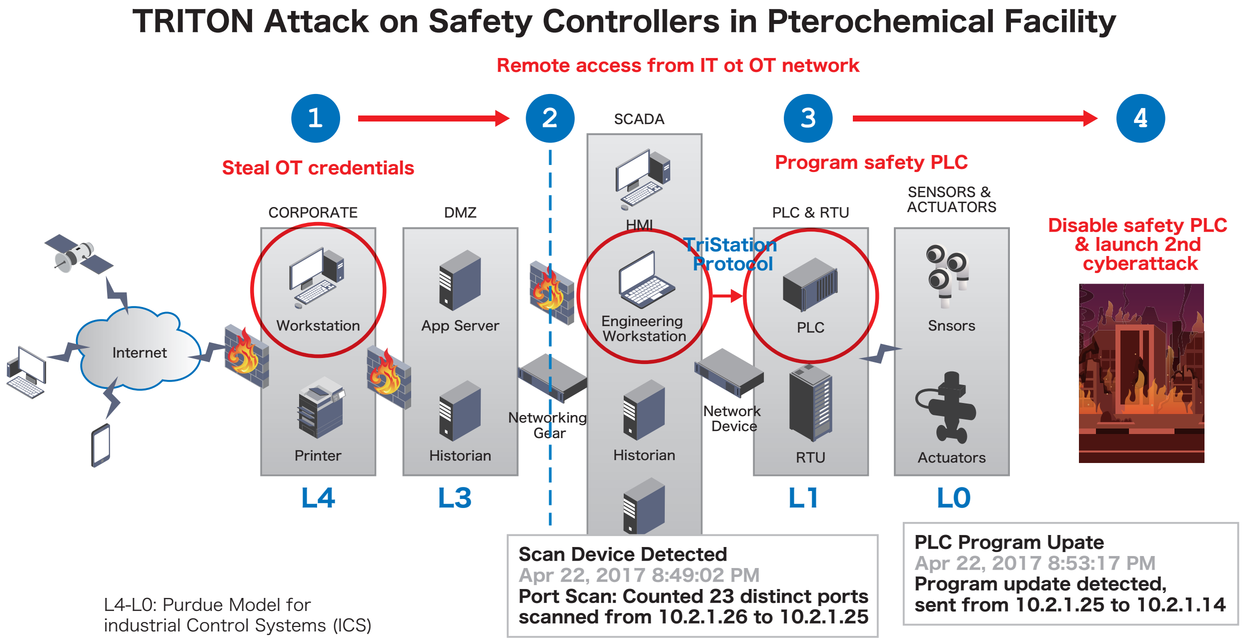


Figure 6-46. Example Diagram of OT Network and Triton/Trisis Attack Targets[247]

[246] https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-trisis-malware-mystifies-industrial-community/#:~:text=TRISIS%20malware%20was%20first%20detected,place%20to%20prevent%20plant%20shutdowns.
https://www.darkreading.com/cyberattacks-data-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known

[247] https://www.sans.org/blog/triton-trisis-in-search-of-its-twin/



Scan Device Detected
Apr 22, 2017 8:49:02 PM
Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25

PLC Program Upate
Apr 22, 2017 8:53:17 PM
Program update detected, sent from 10.2.1.25 to 10.2.1.14

Figure 6-47. Purdue Model of Triton/Trisis Attack Targets[248]

In 2017, the world learned about an unprecedented intrusion into the industrial safety systems of a Saudi Arabian refinery. According to United States Department of Justice indictments[249], the intrusion dated back to at least August 2014 when attackers associated with a nation state targeted energy facilities in the United States and across the globe. The timeline of the attack, its associated steps, and offer insights into how forensic investigators might collect and evaluate evidence in complex attacks against IT/OT environments.

- In 2014, attackers breached access to computers within the refinery and established a foothold.

This foothold allowed attackers to perform detection testing- they uploaded modified open source security tools (including cryptcat) to establish communications and begin to access and build capabilities against the industrial process within the refinery. Note: a gap in open reporting exists between 2014 and 2017.

- In May 2017 the attackers were again observed uploading cryptcat and accessing technical files associated with the safety system.

From a forensic perspective, responders built the timeline from 2014-2017 through MACB file modification records on the uploaded binary.

- In late May 2017, attackers began researching specific out-of-date historian software present within the environment.

[248] https://www.microsoft.com/en-us/security/blog/2020/11/25/go-inside-the-new-azure-defender-for-iot-including-cyberx/

[249] https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

Within industrial environments, historians keep records of certain process characteristics both for performance evaluation and compliance. As historians are often accessed by users both in the industrial plant and outside the industrial plant or refinery, historians often serve as a pivot point and are allowed through many industrial cybersecurity firewalls and monitoring tools. In researching the historian software, attackers gained deeper knowledge into the log file format of the safety system within the refinery.

- Attackers elevated the campaign further on May 29, 2017 when they were observed accessing an engineering workstation via stolen credentials and placing a backdoor for future access.

In the context of industrial networks, engineering workstations are most commonly older Windows systems containing software for configuring both embedded industrial devices and other parts of the industrial process. Engineering workstations possess the software to make significant changes to the environment and are where such changes originate. The expected nature of an engineering workstation making process modifications might be present in the device' s network profile, but devices capable of differentiating between maintenance windows and production windows should trigger based upon such network traffic. As an engineering workstation is often a Windows system, any present forensic evidence aligns with any other active directory domain-joined machine.

- On June 2, 2017, attackers pivoted to an embedded safety system attack, bypassing the physical program key on the safety system.

Many safety systems have a physical key enabling the safety system to be set in "Off," "Program", or "Run" states. In the Off state, the safety system does not run applications. In the Run state, only applications on the device run; however, certain changes are restricted. In Program state, the process doesn' t run but configuration changes may be made. In the case of the safety system targeted by attackers, the physical key was present but the safety system relied on a software register, and the key only drove the state of that software register. The attackers patched the legitimate binary to allow them to remotely turn the Triconex device to Program mode irrespective of the physical state of the key.

While the previous stages of the attack aligned with the typical capabilities and behaviors of an attacker targeting Windows endpoints, the pivot in this stage represented a significant shift in sophistication. Safety systems are embedded devices that are not simply logged into. Developing such a capability requires both software and hardware reverse engineering skills. The acquisition and configuration of a safety system also requires significant capital and knowledge. While programmable logic controllers can easily be found on eBay and other websites, finding and piecing together an entire safety system is very difficult. The attackers also had to have enough network awareness to know which system to target. From a forensics perspective, it is also challenging to get access to the operating system of the safety system, which runs real time operating systems.

- On July 17th, 2017, attackers installed keyloggers to collect user login credentials. In August 2017, attackers pushed a sophisticated industrial-focused capability to the safety systems at the refinery.

On August 4th, 2017, after attackers had rolled out the safety system malware across a number of safety systems, one of the devices triggered a fault due to a bug in the malware, causing an emergency shutdown of the refinery. The attackers continued to access business systems within the targeted organization to understand incident response techniques. This malware, later dubbed Triton/Trisis/Hatman, represented the first time that a publicly known intrusion into a safety system occurred. Prior to this event, other notable major industrial events included the Stuxnet virus which targeted Iranian Nuclear enrichment between 2005-2010 and intrusions into Ukraine' s power transmission and distribution substations in 2015 and 2016. Many other intrusions also occurred that did not cause industrial impact but led to an industrial site being breached.

Incident responders and investigators should note a few major characteristics of this intrusion.

First, the intrusion started with a combination of spear phishing and targeting traditional Windows systems.

Second, this attack occurred over a timeframe of years, including a significant knowledge gap between forensic evidence collected in 2014 and when activities ramped up in 2017. The attackers did not simply gain access and elevate in the same day.

Third, the amount of preparation, planning, and development by the attackers was significant. The attackers gained access for years to study both the technical and operational aspects of the business. Log file formats and information about the target' s particular systems served as key data points for this operation.

Fourth, while the attackers did perform some of this research in the targeted environment, they almost certainly had access to test environments where they could build malware for the embedded safety system and perform detection engineering testing. While the attackers did ultimately make a mistake, they were able to successfully dwell in the environment for years with traditional malware and for months with specialized malware for the specific safety system.

Fifth, the threat was found not because of network or host detection, but rather due to the failure of the industrial malware itself. Many industrial environments use passive network monitoring which is easy to implement and relatively low maintenance. Trisis evaded detection with cryptcat (among other methods), proving that passive network monitoring alone struggles to detect such attacks in many ways. The host-based indicators served as the only source for investigators to reconstruct a timeline of events. When performing evidence collection, it' s important to realize what network and host sources are available in an environment and when additional collection should be deployed to build a more complete timeline.

The 2017 Trisis breach into the Saudi Arabian oil refinery represents an amazing case study of both intrusions into industrial operations and the importance of collecting both host and network data when dealing with breaches into environments with both traditional and embedded devices. While a sophisticated and well-resourced attacker executed this breach, many of the techniques observed represent common attacker tactics, techniques, and procedures that may be the focus of many investigations.

Chapter 7

Methods of Evidence Analysis

Introduction

In the “Methods of Evidence Analysis” knowledge domain, evidence is aggregated and analyzed through specific examination methods. Cybercrime investigators never treat evidence as coincidence – cybercrime investigations require analysis controls based on data science. These controls must be defined as essential elements in effective evidence analysis frameworks and include testing, quality assurance, and disclosure of results.

Through this knowledge domain, cybercrime investigators can consider cybercrime by “scope”, “stage”, and “type” to identify risks and threats related to an organization. The domain also includes "profiles" of "threat actors" (cyber criminals who give rise to threats to enterprises and organizations) and impact analysis regarding the "activities" that they perform.

This knowledge domain provides cybercrime investigators with essential fundamental frameworks for developing effective methods of evidence analysis. These frameworks also help managers define "policies", "systems", and "procedures" related to prevention and protection.

This knowledge domain is divided into three topics closely related to "Sources of Evidence" (Chapter 5) and "Methods of Evidence Collection" (Chapter 6): aggregation, analysis framework, and interpretation of results. Just as the collection of appropriate evidence from available sources is important for cybercrime investigators, evidence analysis is important for evaluating the scope of cybercrime. In general, investigations have constraints, and technology and other resources should be allocated in accordance with the evaluated scope to drive efficiency and effectiveness in evidence analysis. .

The “Methods of Evidence Analysis” knowledge domain is related to all other aspects in cybercrime investigations and cybercrime investigation knowledge domains in this document. Learning this knowledge domain will allow readers to acquire an understanding of the following:

- How should evidence be aggregated and analyzed for the purpose of cybercrime evidence analysis?
- How should efficient data management and analysis frameworks be defined?
- How should analysis results be recorded and associated with the scope of the cybercrime?
- How should impact analyses related to "threats," "activities," and "threat actors” be interpreted?

Topic in Methods of Evidence Analysis

Figure 7-1 displays topic categories in the “Methods of Evidence Analysis” knowledge domain.

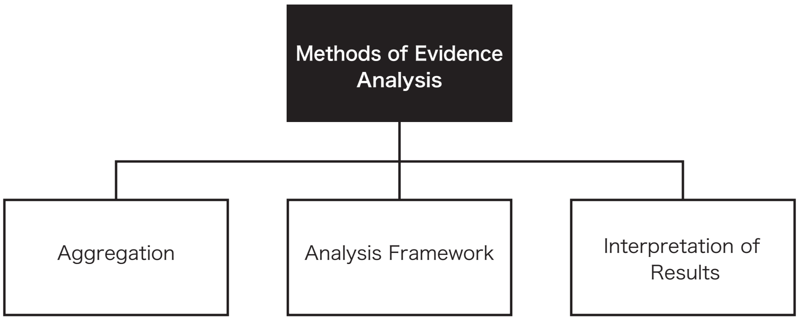


Figure 7-1. Topic Categories in the “Methods of Evidence Analysis” knowledge domain

Aggregation

Aggregation deals with definitions of "Collected Evidence", "Threat Intelligence", and "Data Elements in an Investigation". In many cases, it is difficult to demonstrate facts only using singular pieces of information scattered throughout cyberspace. As a result, multifaceted aggregation of fragmented singular pieces of information is essential. Aggregating the evidence collected in cybercrime investigations allows it to be sublimated into "Threat Intelligence", which in turn creates a decision-making cycle based on the information.

Collected Evidence

"**Collected Evidence**" is the collection of foundational evidence to identify an individual or organization that has committed or participated in a wrongful act.

Collected evidence can be divided into two categories: "**personal evidence**", which is the testimony of witnesses, experts, and involved parties, and tangible "**physical evidence**".

When collecting either type of evidence, it is essential to understand its use in future legal proceedings. In other words, evidence must be collected using only appropriate and legal means. Investigators should be able to prove that collected evidence has not been altered to guarantee its credibility.

In cybercrime investigations, all-important "electronic data" is subject to " **Volatility**" which is not found in tangible documents. The admissibility of such evidence may be forfeited if it is lost or altered due to mistaken operations. For this reason," **CoC (Chain of Custody)**" is an important concept and procedure in cybercrime investigations.

CoC requires a description of all people who have been able to access and handle the evidence. This mechanism guarantees the credibility of evidence by clarifying when and where evidence was collected, where it was stored, and who safeguarded and managed it. Refer to the "Methods of Evidence Collection" knowledge domain (Chapter 6) for specific details regarding the CoC in cybercrime investigations.

It is also important for investigators to understand the difference between collecting evidence as part of an official investigation and collecting telemetry to support detection and response activities. Figure 7-2 illustrates the DFIR process. As shown below, the detection stage comes first and, as a result of an identified breach, an investigation might be initiated as part of the response. At the detection stage, analysts use telemetry available through various controls and mechanisms such as EDR tools but there is no requirement for the telemetry to be collected and verified in a way that it is court admissible. On the other hand, during the investigation stages, appropriate measures need to be taken to ensure evidence is collected properly as described in Chapter 6. Thus, telemetry that can be used for detection is not always admissible evidence. Such issues need to be considered in the forensic readiness plan of each organization.

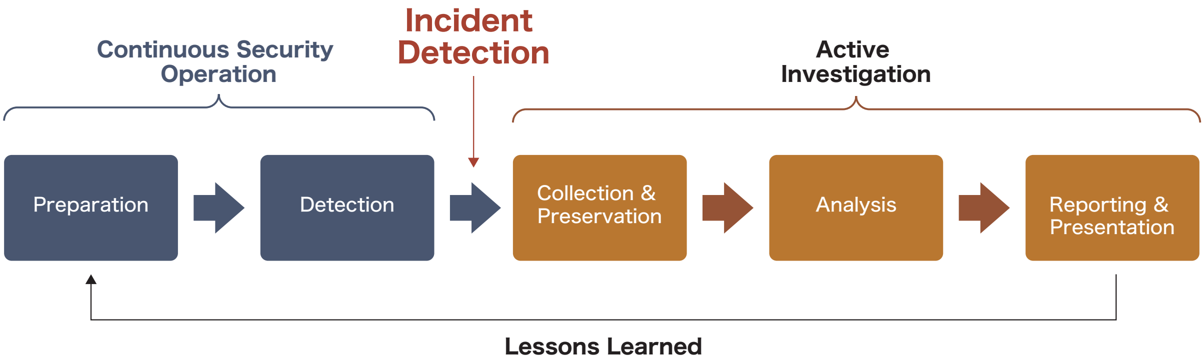


Figure 7-2. DFIR process

Threat Intelligence

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is information derived from collected, processed and analyzed data that relates to threat actors and their motives, goals, targets, and techniques. TI allows organizations to prepare, defend, and respond against cyber incidents and cyber assisted crimes.

As shown in Figure 7.3, the lifecycle of TI begins with the identification of the type of intelligence to collect (Planning & Direction phase). Next, **raw** data is collected during the Collection phase. Raw data simply presents facts demonstrated through nothing but numbers, characters, diagrams, images, sound, and so on. These data points can derive from a variety of **sources** that may be external or internal to an organization, or publicly available or closed, and so on. However, raw data is not directly usable and a number of different techniques must be used to process, transform, structure, and enrich it to extract **information**. In doing so, information must be processed to allow the application of analysis methods (Processing phase). During the processing phase, various methods are deployed,- from manual processing and curation to natural language processing and machine learning techniques. Once information is processed, the analysis (Analysis phase) of information produces **knowledge** and the identification of patterns, trends, and insights that can be disseminated and consumed by different functions of an organization (Dissemination phase). Finally, **wisdom**- higher data quality- can be achieved to make informed decisions and actions. These concepts are also presented in the Data Information Knowledge Wisdom Pyramid (DIKWP) in Figure 7-4. It is also worth noting that threat intelligence can be collected during one step of an investigation to be used in a later step.

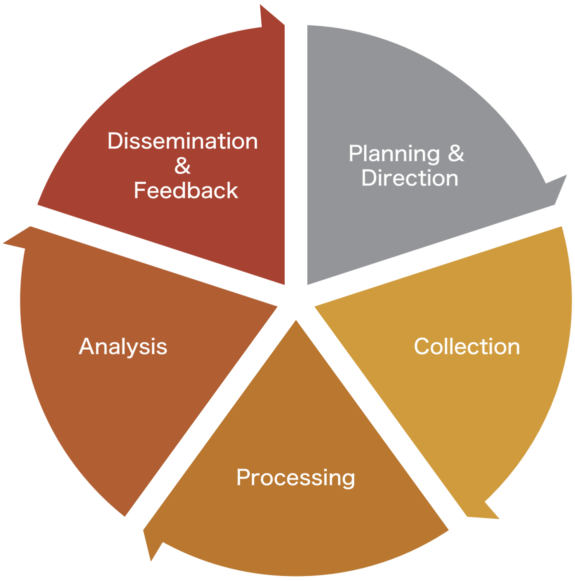


Figure 7-3. Threat Intelligence lifecycle

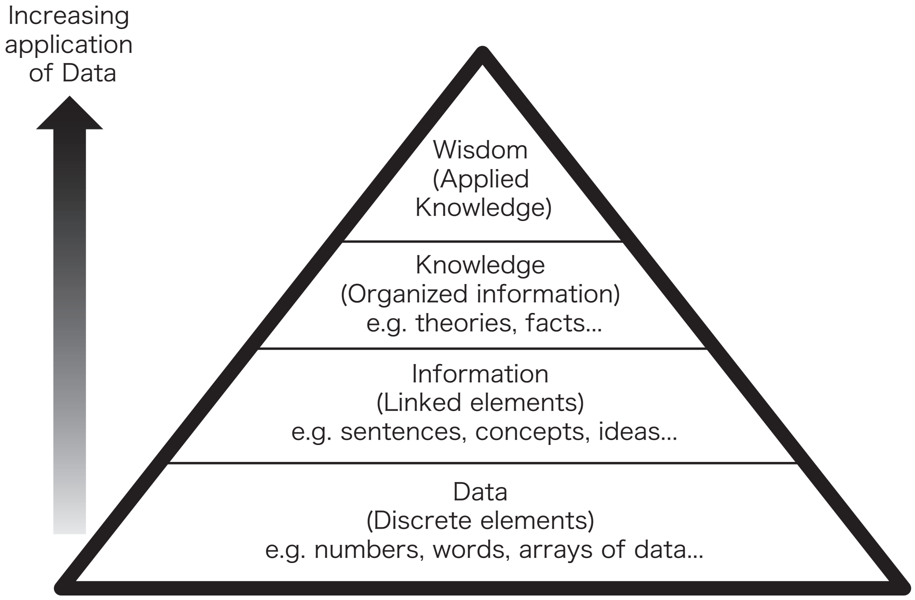


Figure 7-4. DIKWP pyramid

As mentioned previously, threat Intelligence can derive from internal or external sources. Internal intelligence might be produced from previous or current incidents and investigations, collected evidence, or existing knowledge about the organization. External intelligence may be sourced from publicly available or proprietary/commercial platforms. External intelligence usually provides a larger variety of information that is less relevant to a company- for example, if a similar incident impacted similar (but not identical) organizations. On the other hand, internal intelligence tends to provide a lower volume of information with higher fidelity and quality. However, there is one type of external intelligence directly related to a company which can significantly benefit a forensic investigation and the overall posture of a company: brand intelligence. Brand intelligence refers to the process of monitoring external intelligence for risks directly affecting a company such as leaked credentials, compromised assets, expired certificates, or data leaks.

TI can be categorized into three types of information: Indicators of Compromise (IOC); Tactics, Techniques, and Procedures (TTPs); and Situational. **Indicators of Compromise (IOC)** refers to fragments of information that indicate a system might have been compromised. IOCs can be sourced externally or identified during an internal investigation. IOCs vary from hashes of malicious files and network connections to known bad IPs and registry keys used by threat actors for specific purposes. It is important to note that the value of such indicators fades over time. An investigator or analyst should always apply critical thinking and use the properties available for each IOC to determine if it is applicable to the investigation. For instance, an IP might have been identified as malicious one year before the incident under investigation, which would make the value of the IOC low.

Each IOC is associated with various properties. Multiple formats have been proposed and are used for IOCs. Investigators should use a combination of formats to guarantee comprehensiveness. Typical IOC formats include:

- STIX (Structured Threat Information eXpression)
- MISP (Malware Information Sharing Platform & Threat Sharing)
- YARA (Yet Another Recursive Acronym)
- CybOX (Cyber Observable eXpression)
- OpenIOC (Open Indicators of Compromise)
- TAXII (Trusted Automated eXchange of Indicator Information)

Tactics, Techniques, and Procedures (TTPs) is a term originating from the military and intelligence analysis that has been introduced in cybersecurity. **Tactic** refers to a threat actor' s tactical goal: why they are performing an action. **Technique** represents how the activity is performed: for instance, a threat actor might use an existing command and control channel to exfiltrate data. **Procedures** are used to describe specific implementations of techniques. The most well-known and used knowledge base of TTPs is MITRE ATT&CK[250] (Adversarial Tactics, Techniques, and Common Knowledge) which was introduced in 2013 by The MITRE Corporation.

Situational intelligence represents abstract information, such as trends observed over time and geopolitical situations.

[250] https://attack.mitre.org/

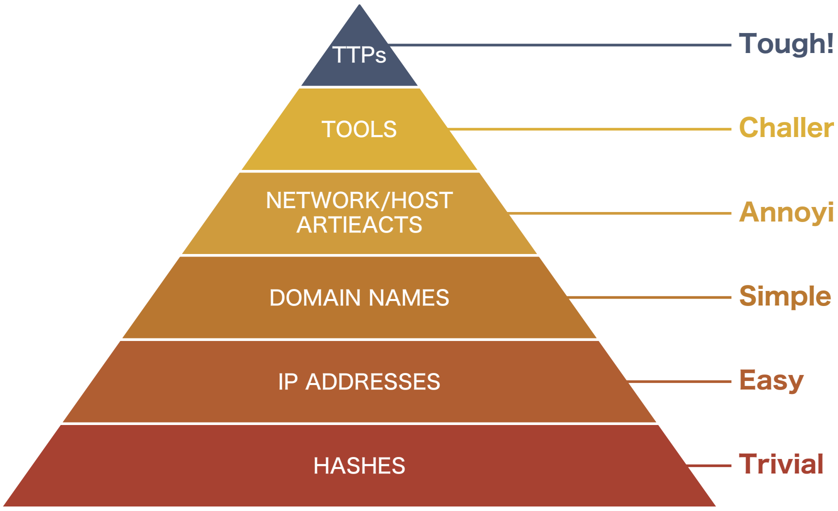


Figure 7-5. Pyramid of Pain

However, not all types of TI have the same value. The **Pyramid of Pain**[251], created by David J Bianco (Figure 7-5), represents how different types of indicators and knowledge vary in value, applicability, and difficulty in sourcing and changing. This does not mean that one type of indicator is better than the other, as each has its advantages and disadvantages and is meant to be used in different ways for different functions.

Specifically, the lower levels of the pyramid include indicators that are easy to collect but less valuable, like hash values and IP addresses. Though these indicators are easy to identify, they lose their value very easily. For example, an attacker can simply modify the hash of a malicious file to make the indicator obsolete. The middle of the pyramid contains network and host artifacts and tools. The former may include network protocols, user agents, and registry keys or directories, while the latter includes the actual tools and utilities used by threat actors to achieve various tasks such as lateral movement, the exfiltration of data, and so on. While these indicators are harder to collect as they require analysis, they are also harder to modify as they require resources such as money or time to buy or develop new tools and new campaigns to disseminate them.

TTPs sit at the top of the pyramid as the toughest indicators to collect, as they not only represent the technical details a criminal may use but also their overall methods, aims and goals. As explained, TI can be applied in multiple operations and activities for any organization. Different types of threat intelligence can support different functions, and can be classified into four functional categories: operational, strategic, technical, and tactical.

- **Technical** Intelligence is focused on information such as IOCs and vulnerabilities. It is meant to be used mostly by Security Operation Centers and other technical teams for detection, analysis, and response.
- **Tactical** Intelligence represents urgent threats that need to be immediately mitigated and actioned, such as new vulnerabilities.
- **Operational** Intelligence focuses on information on the higher level of the pyramid, i.e. TTPs. This type of intelligence can be consumed by many different functions, from threat hunters and

[251] https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

content developers to forensic investigators.

- **Strategic** Intelligence represents a broader view of the threat landscape including situational intelligence and emerging threats and trends. It can support an organization' s stakeholders making intelligence-driven decisions and managing risk.

Data Elements in an Investigation

There is a fundamental difference between forensic investigations and the rest of the detection and response functionalities of cybersecurity: the output and methodology in forensic investigations needs to be documented in a way that can be presented in a court of law. This section presents the most important data elements included in fully or partially digital crime investigations, as shown in Table 7-1. The accumulation of data as IOC is essential to all of these elements.

Table 7-1. Data elements accumulated as IOC

Data elements to accumulate as IOC	
Victimology	Why was the victim harmed in the crime?
	Was the victim known to the attacker?
	Is there some kind of possibility that the victim was able to be targeted?
	What type of risk did the attacker take in committing the crime?
Crime Scene Indicators	Scene of the crime
	Time of the crime
	Crimeware
Forensic Finding	Data forensics
	Application forensics (including the results of reverse engineering)
	Network forensics

●Victimology

“**Victimology**” is profile information related to the victim. It is important to examine why the victim was the target of the crime. If data or infrastructure was damaged by cybercrime, it is important to record it (including targeted digital assets). Focusing on victimology allows investigators to evaluate the reason the victim was targeted and makes it possible to obtain information leading to the attacker's motive. Collecting information about the victim allows an investigator to correlate the victim' s profile with threat actor profiles and TTPs. This can increase resource usage efficiency, improve response time, and support attribution.

The following four questions are particularly important to ask when analyzing cybercrime:

1. Why was the victim harmed?
2. Was the victim known to the attacker?
3. Is it possible that the victim was targeted?
4. What type of risks did the attacker take in committing the crime?

Benjamin Mendelsohn demonstrates methods of victim classification[252] based on the "**Culpability**" of

[252] Benjamin Mendelsohn, “Une nouvelle branche de la science bio-psycho-sociale: la victimologie,” Revue Internationale de Criminologie et de Police Technique, vol.10, 1956, pp.95-109.

the victim, as illustrated in Table 7-2.

Table 7-2. Classification methods based on victim "culpability(culpabilité)"

Degree of responsibility	Summary
Victims with absolutely no responsibility	Infants involved in infanticide or kidnapping, indiscriminate bombings, etc.
Victims with little responsibility	Passive involvement at a crime scene. Victims who induced the malice of the attacker through insults which caused psychological pain, victims of sexual assault who could have easily sensed danger and escaped, but proceeded towards the scene of the crime, etc.
Victims who have the same level of responsibility as the attacker	Voluntary involvement at the scene of the crime. Murder victims who consent to or request their murder, murder/assault victims resulting from quarrels and mutual provocation, etc.
Victims who have more responsibility than the attacker	Provocation by the victim is deemed the primary cause of the attack. Murder/assault victims who are attacked due to threatening to kill the other party' s family, etc.
Victims who have the most responsibility	Those killed/assaulted as a result of self-defense carried out due to an unlawful attack.

●Crime Scene Indicators

"**Crime Scene Indicators**" are the elements which comprise a crime scene. It is important for investigators to understand the key points to focus on once they lock down the crime scene.

✓Crime scene:

Many cybercrimes are built up through a division of labor using experts in respective fields. As a result, one incident may straddle multiple fields. For example, an illegal information trading incident using malware will feature the development base of the malware, the website tampered with to become a stepping stone in the distribution of the malware, the botnet used to maliciously distribute spam for the purposes of spreading the malware, the Command and Control (C&C) Server used by the criminal, the host computer infected by the malware, and the market in which information stolen from the computer is bought and sold. This represents at least six crime scenes to assess.

Cybercrime investigators should not only have a full understanding of physical locations but should also gather and record digital identification information (MAC addresses, IP addresses, digital certificates, URLs, network addresses, Internet Service Providers, etc.), and characteristics of services found at the crime scene (free, paid, information required for registration for use, etc.).

✓Time of the crime:

It is possible to obtain insights related to the motives and behavioral patterns of the criminal based on the time of the crime. Moreover,, it is also possible to evaluate timelines to gain an understanding of the criminal' s degree of skill, risks regarding the crime, the likelihood of obtaining more evidence, and so on.

Logs are beneficial to cybercrime investigators and specify the time of the crime. Logs can be divided into "security software logs" which include information related to computer security, "operating system logs" which contain system usage logs, and "application logs".

The possibility of discrepancies in timestamps should be considered when software logs are handled. Software logs reference the clock of the host computer on which they are stored to set timestamps for all log items. Therefore, if the clock of the host computer is inaccurate the timestamps of the logs will also be inaccurate. Specifically, if there are discrepancies in timestamps when analyzing logs obtained from multiple hosts, investigative insights regarding the incident may be far from the mark if investigators aren' t careful.

Additional information related to the time of the crime may be gained through malware analysis and computer forensics.

✓ **Crimeware:**

“**Crimeware**” is a general term for software created or used for criminal acts. A popular example is "**Malware**", malicious software created with the intent to perform wrongful or harmful actions. However, software that should be considered in cybercrime is not limited to malware. Investigators should also consider that software created for lawful purposes and software belonging to operating systems are sometimes misused in criminal acts. Therefore, cybercrime investigators must first identify whether the crimeware they are investigating existed at the crime scene previously or was brought in by the criminal.

For example, a criminal who successfully breaks into a network will use standard commands on Windows OS such as tasklist, ver, ipconfig, and systeminfo to collect information (processes information, network information, OS information) from the infiltrated host computer. These are not pieces of software that the criminal has brought in- they are pieces of software that existed at the crime scene previously. This technique is called Living off the Land (LotL) and is commonly used by criminals to blend their actions into legitimate operations and stay undetected for longer.

An additional critical trend is that modern software is not necessarily managed and used via the host computer- it is often cloud-based. "**Cloud computing**" is widespread and entails services that are used via networks such as the Internet. The four most common cloud computing services are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Function-as-a-Service (FaaS). Different types of cloud computing provide different levels of control and ownership. It is therefore important for investigators to understand cloud technologies to collect and analyze corresponding evidence and to account for their limitations.

Investigators may encounter cases in which the software used in cloud environments is misused as crimeware, in addition to cases in which identification is difficult because physical access to cloud computing is impossible (which results in no evidence at the crime scene). Even in these challenging situations, accurate reproduction and analysis is possible through cache information in the browser utilized for the cloud service and in the temporary files generated on the host computer for cloud computing access. It is also possible to obtain IOCs through approved methods which enable investigative conclusions. In addition, it is possible to obtain further IOCs through an analysis of programs which comprise software. Specific details for these methods can be found in the "Forensic Finding – Application Forensics” section below.

●Forensic Finding

"**Forensic Finding**" refers to a discovery obtained when analyzing "physical evidence" related to the crime, in order to legally prove the occurrence of the crime. This discovery becomes data that supplements "Victimology" and "Crime Scene Indicators." It demonstrates the objective facts of the crime's characteristics and becomes a verified IOC, which is held in the highest regard.

For sequential discoveries, it is essential to protect the integrity of information by maintaining strict data safeguarding and handovers.

Digital forensics can be divided into three categories in accordance with the data being analyzed:

✓ Data forensics:

The targets of analysis are file storage media, file systems, or files used by digital devices (including mobile and IoT devices). File systems must be considered when analyzing the data, and can preserve deleted files and the history data of existing files. This data may contain extremely important information for the cybercrime investigation.

✓ Memory forensics:

The targets of analysis are memory dumps collected from digital devices at a specific point in time. Memory dumps contain a variety of information, from active processes and network connections to malware injected in processes and cryptographic keys. It is important for the memory to be collected as soon as possible to preserve data, due to its volatile nature.

✓ Cloud forensics:

The targets of analysis are cloud environments. In some cases, cloud forensics includes one or more of the forensic findings and procedures mentioned in this section. For instance, it may include a file disk analysis of a Virtual Machine hosted in the cloud or cloud specific logs. Similarly, authentication logs from cloud environments could be considered application forensics. Regardless, cloud forensics should be considered a separate category due to the increasing adoption of cloud computing and subsequent challenges which should be taken into consideration in forensic readiness preparations.

✓ Application forensics:

The targets of analysis are programs including OS (operating systems). The volatility of associated data must be considered during analysis- since volatile data may change over time, sequence and chronology are important during collection.

Furthermore, by using the three methods presented in Table 7-3 to analyze programs which comprise software, investigators may discover new IOC:

Table 7-3. Program analysis methods

Analysis method	Description
Surface analysis	Checking the information recorded in files without running the program
Dynamic analysis	Checking operation by actually running the program together with tools such as a debugger
Static analysis	Analyzing the source code Checking functions at the code level through reverse engineering techniques such as disassembly and decompiling

Examples of IOC obtained from this analysis include Mutex, which prevents multiple instances of programs running, and information which functions as a program such as URLs targeted as C&Cs, HTTP requests strings disguising browser communications, and HTTP response strings disguising servers.

In addition, if the time when the program was compiled can be identified, it may be possible to hypothesize the time at which the crime was planned and the time zone where it was committed (the location of the crime). Furthermore, when analyzing Strings information (extracted as ASCII characters from within programs) can enable hypotheses regarding the identity of the criminal, including the criminal's development environment and languages of use (computer languages or spoken languages).

✓ Network forensics:

The targets of analysis are packets which travel through the network. The layer structure in each protocol suite must be considered when analyzing this data. In many cases, relevant activities are found in the layer closest to the user (victim or criminal) – the application layer.

Analysis Framework

Analysis Framework deals with definitions of "Data Modeling", "Data Mining", "Extraction, Transformation, and Loading", "Data Quality Testing", "Automation", and "Quality Assurance and Control."

In a modern world which increasingly relies on cyberspace, obtainable electronic data continues to diversify in not only cybercrime but traditional crime as well. In such an environment, investigators in charge of data analysis must find data of value within large amounts of data using a scientific "Analysis Framework". Utilizing an analysis framework in cybercrime investigations allows the primary factors in the background of the crime to be identified. As a result, a decision-making cycle based on information is established.

Data Modeling

"Data Modeling" refers to the technique of representing data, in a structured way, as a set of objects and their relationships with each other based on defined rules. This process involves the definition of entities, attributes, and relationships between entities as well as constraints.

In police activities, data-based data modeling should be carried out for the purpose of supporting the overall investigative mission. It should help investigators make hypotheses regarding "threat actors" and reasoning regarding causal relationships in the "activities" they perform. Data modeling can also help investigators identify f relationships that were previously unknown, as well as support further processing and visualization in a more efficient way. However, modeling is not limited to the technical analysis of an investigation. Modeling can also be utilized by managers in areas such as budget planning and police policy.

Table 7-4 illustrates the merits of performing data modeling in police activities:

Table 7-4. Merits of data modeling in police activities

Optimization of police activities	Optimized resource allocation
	Evaluation and prioritization regarding investigative scope
Incident resolution	Hypotheses regarding "threat actors" and arrests
	Prosecution of criminals
Improved public order	Information provision to citizens and public awareness
	Strengthened patrolling for areas predicted to be dangerous
Future crime prevention	Planning for essential resources
	Development of effective strategies and tactics
	Policy recommendations
	Lessons learned

●Data Types

Various types of data are handled in criminal investigations. However, data can be broadly classified into three main categories: "**structured data**", "**semi-structured data**", and "**unstructured data**".

Table 7-5. Structured data, semi-structured, and unstructured data

Structured data	Data organized in a predefined and well-structured format. Examples of such formats are databases and spreadsheets, which all have categorized elements and allow the definition of the relationship between those elements.
Semi-structured data	Data that is not organized in a formal structure such as a database but still follows a hierarchy and some level of structure. Examples of semi-structured data include XML and JSON files, which are commonly used for event logging on various systems.
Unstructured data	Data not formatted in a structured way that cannot be handled in a defined manner. Examples include documents, email, photos, and videos.
Future crime prevention	Planning for essential resources

For example, imagine a drug trafficker is arrested and his computer is seized. As a result of analysis to email records (unstructured data) on the computer, several suspicious exchanges are identified. Furthermore, restoration of deleted files from the seized computer is attempted. As a result, spreadsheets indicating dates, names, and prices are discovered (structured data). Extending the operation to identify the drug sales network then becomes possible.

While processing structured and semi-structured data can be achieved using various methods with ease due to their structure, it is evident that the opposite applies for unstructured data. Consequently, pre-processing is required to enable an accurate interpretation of the meaning of documents and information on a computer, and must be performed before the data is organized. There are many methods to support the processing of unstructured data, such as:

- **Metadata extraction:** Metadata is not the data itself; it is associated information describing information about the data in question. Types of metadata and examples are described in Table 7-6.

- **Text Mining**: Also referred as texted analytics, text mining includes the processing of text data with the aim of extracting insights and information which can then be further processed using other methods in this list.

- **Image** and **Video analysis**: This focuses on the processing of images and videos to extract and interpret structured data. Image and video analysis includes techniques such as optical character recognition (OCR), image classification, and object detection.

- **Audio analysis**: This involves the processing of audio and spoken language in order to then apply other methods, such as speech recognition and audio classification, for further analysis.

- **Natural Language Processing** (NLP): This focuses on linguistic analysis with the aim of "understanding" in the same way a human would. It should be noted that even though NLP is widely used along with text mining, it is not limited to this type of data and can be applied to other pre-processed data such as images and audio. Other tasks such as **Sentiment** analysis and named entity recognition (NER) are often included in NLP.

- **Machine Learning** and **Data Mining**: While both of these fields use algorithms to analyze and extract insights from data, machine learning aims to learn from the data and make predictions or decisions, while data mining aims to explore the data, discover patterns, and extract information. Both fields support many of the other methods of unstructured data analysis and will be discussed later in this section.

Table 7-6. Types of metadata

Type of metadata	Description	例示
System metadata	Information handled by file systems, including type, size, date created, owner, and access privileges	・Exif, which is found in digital photo files ・Properties and personal information in Microsoft Office files (Word/Excel/PowerPoint)
Custom metadata	Information associated to data, such as time and date, recipients, etc.	・"To" and "From" fields in call logs and email ・Conversation times in call logs ・IMEI information in mobile phones
Rich metadata	Information converted to text through image OCR and voice recognition	・Information from voice conversations converted to text ・Text information, including screen captures

Data Storage and Management

Data storage is a critical part of not just forensic investigations, but information systems in general. Both **Data Lakes** and **Data Warehouses** can be used for this purpose. The main difference is that while Data Lakes allow the storage of raw unstructured data, Data Warehouses can only be used to store structured data that has been previously cleaned, transformed, and processed if necessary. This section will focus on Data Warehouses, as they are more often suited to support the requirements of investigative systems due to:

1. The ability to support historical data management and trending.
2. Increased analysis (query) performance compared to data lakes, due to the use of only structured data.
3. Data consistency and quality which fulfill requirements for integrity and accuracy.

A "**Data Warehouse**" is a large-scale database that stores data which is extracted and rebuilt from multiple information sources and is used for information analysis and decision-making. Proponent William H. Inmon defines a data warehouse as "a subject-oriented, integrated, time-variant and non-volatile collection of data in support of management's decision making process".

Thus, the three main characteristics of a Data Warehouse are "time variance", "subject orientation", and "integration". Since system resources are limited, it is not possible to continually collect "**transaction data**" related to all crimes on one system. Consequently, when constructing real-world systems, it is common to build systems which collect data by periodically refining it from a viewpoint which considers the speed at which necessary data can be obtained, and to build systems by individual function from a viewpoint which considers efficiencies such as work specialization. These types of systems provide excellent convenience.

However, in the locations where cybercrime investigations occur, there are times when crime trends must be analyzed from a long-term perspective. In these situations, databases which do not contain past data cannot be used for the analysis of crime trends. Therefore, Data Warehouses must also store past data sequentially- this is referred to as "**time variance**".

In addition, cybercrime investigation databases are built by classification. This involves building databases for each IOC such as "IP address", "URL", "WHOIS", and "malware hash values", along with "Threat Actors", "Modus Operandi", and "TTPs (Tactics, Techniques, and Procedures)". Since each data format, serial number, and son on differs per system, the data cannot be used as it stands. Therefore, it is integrated by type, such as "incident" and "criminal group". In a Data Warehouse, this is the "**subject-oriented**" organization. Finally, collecting and combining data distributed across different systems into one database is called "**integration**".

The methodology that enables the storage of data in a Data Warehouse is called "**ETL (Extraction, Transformation and Loading)**". ETL is the sequential process of "**Extracting**" data from a source such as NIBRS (National Incident-Based Reporting System), "**Transforming**" it as needed, and "**Loading**" it into a target system such as a Data Warehouse. Note that due the order of operations, all data at the end of the ETL process is structured, and thus, storing data in a data warehouse instead of a data lake is the optimal choice.

●Extraction

In the "Extraction" process, data is extracted from the system (the source of the information) and transformed into a state in which it can be processed. This process is called instantiation. Through instantiation, information such as field type and value are imported and can then be specified. There are times when, as a result of decision-making and data collection which use modeling, data extraction is reconsidered.

Information sources in criminal investigations include incident data, report data from related organizations, jurisdictional data, and personal data, as well as data related to organizations such as criminal history, data, and so on obtained from police activities. Depending on the organization, data stored in a database such as “RMS (Records Management System)”. For specific sources of information in criminal investigations, refer to Chapter 5: Sources of Evidence.

✓ Incident data: “Incident Crime Report”, “Arrest Reports”, and “Call for Service Records”
✓ Report data from related organizations
✓ Jurisdictional data
✓ Data related to individuals or organizations, such as criminal history
✓ Data obtained through police activities

● Transform

In the “Transform” process, data extracted from multiple information sources is combined then processed according to fixed rules, or rejected if it is fraudulent. This process includes data selection, organization, compilation, combining, and format setting.

✓ Combining data from different systems
✓ Standardizing field values of differing types
✓ Defining values for deficiency, fraudulence, and extremity
✓ Data selection
✓ Recompiling data in formats required for analysis
✓ Transforming related fields

● Loading

In the “Loading” process, data files created in the “Transform” process are imported into a data warehouse. The process creates databases for information analysis and decision-making.

Machine Learning and Data Mining

“Machine Learning” and **“Data Mining”** are both fields that support the analysis of large datasets and increase efficiency in forensic investigations. The terms are often confused and while they differ in nature, they work synergistically when combined. **“Machine Learning ''** is a branch of artificial intelligence which uses (trains) algorithms to learn from data and predict and classify with a high degree of accuracy. This allows such algorithms to predict or take action without the need for explicit programming. Machine learning algorithms are utilized for various types of analysis (many described earlier in this chapter), one of them being Data Mining, which will be further explained below.

In Machine Learning, algorithms are trained on datasets. Datasets can be labeled, where each data point has an output label assigned to it, or unlabeled. Models go through a ”training” phase in which they learn from data before their performance is assessed against a different dataset. The most common types of Machine Learning algorithms are presented in Table 7-7:

Table 7-7. Common Machine Learning algorithms

Model name	Result obtained
Supervised Learning	Models are trained on labeled data and used for applications such as classification.
Unsupervised Learning	Models are trained on unlabeled data with the aim of identifying patterns and structures. Clustering and anomaly detection are examples of unsupervised learning.
Semi-Supervised Learning	Both labeled and unlabeled data are used during training to leverage the advantages of supervised and unsupervised models.
Reinforcement Learning	Reinforcement involves a feedback loop (agent) that provides rewards or penalties. The model learns via a "trial and error" method.
Deep Learning	Deep Learning uses bio-inspired artificial neural networks with multiple layers (deep networks). Image processing, Natural language processing (NLP), and Large Language Models (LLMs) are some applications of Deep Learning.

"**Data Mining**" is the technique of exploring data and mining useful insights and patterns. Investigators in charge of data analysis support and contribute to criminal investigations by taking a large amount of data with no uniformity, converting it into a format that is more easily used, and using statistics-based tools to discover correlations between data and hidden indicators.

In Data Mining using analysis models, analysis is carried out by establishing a hypothesis in advance, then collecting the necessary data. Verification is then combined with projected events, and the appropriate analysis model is selected. Table 7-8 displays analysis models used in Data Mining. Additionally, the tools that are used are displayed in Table 7-9.

Table 7-8. Typical analysis models in Data Mining

Model name	Result obtained
Association Analysis	When X occurs, it is also easy for Y to occur
Classification	From the attributes of X, it can be predicted to be Class C
Clustering Analysis	Aggregation of similar items
Regression Analysis	From the attributes of X, variable Y can be predicted

Table 7-9. Tools used in Data Mining

Tool name	Details
Data visualization ・Histogram ・Scatter diagram	Confirming the presence or absence of outliers by ascertaining data trends or distribution and determining the optimum method of analysis to create reports in a diagram or graphic format.
Responses to diverse data ・Text Analysis, Morphological Analysis ・Spatial Analysis ・Pattern Recognition, Computer Vision	Unstructured data is researched to derive important investigative insights.

In contrast, in Data Mining that uses Machine Learning there is no need for a prior hypothesis. Instead, a computer learns from the data, leading to correlations. Although it is difficult to obtain new considerations and implications from analysis results acquired through Machine Learning, it is already being used in fields which require automation such as determining spam mail and detecting illegal credit card transactions. Machine Learning is expected to be used in criminal investigations fields such as classification, recurrence, clustering, and rule extraction.

Both Data Mining and Machine Learning can be used for various tasks, from image and document processing to behavioral analysis of authentication and application logs. They can help investigators analyze data, identify insights, or reconstruct events from large datasets even if they consist of data formatted in different ways or missing segments. However, it is important to note that results obtained via these analysis models and tools should not be trusted immediately. It is necessary to examine discovered results from the perspectives of "accuracy", "reliability", and "practicality".

Data Visualization

Data visualization, or graph visualization, can be a powerful tool in the analysis and interpretation of findings. Data visualization refers to the construction of graphs that represent data and the relationships within it. Visualizing data can help investigators identify patterns and also understand the impact of an attack or missing data. Some common examples of graphs can be found below:

- **Nodes** represent hosts in a network color coded according to their status (compromised, not compromised, and unknown), and the **links** between them represent communications along the corresponding evidence. By updating the graph, investigators can identify further compromised hosts and potential lateral movement, and assess the impact of the attack.
- User logins and source IP addresses for each login are represented as nodes, and each user is linked to the IP nodes from which she/he authenticated from. Further information could be represented on the graph with different **colors** for the country of the IP. This can allow investigators to spot outlier users that are either logging in from countries outside of the baseline or from too many IP addresses.
- Nodes signify entities and evidence. For instance, consider a Business Email Compromise (BEC) investigation where a graph is used to represent the users involved as well as the evidence of compromise, with links showing the relationship between them. This not only allows investigators to summarize their findings, but also helps them spot gaps in their analysis and build hypotheses.

Finally, **timelines** are another data visualization method that should be part of every investigation. Timelines present findings in chronological order. This serves multiple purposes of analysis, similar to a graph visualization, and also assists in the presentation of evidence and conclusions.

Data Quality Testing

"**Data Quality Testing**" entails scrutinizing the results of criminal investigation and measuring to assess their appropriateness.

Various types of data are supplied from a crime scene. Typical examples are shown below.

- CSV (Comma Separated Values): Text file data with a plurality of fields separated by the comma symbol
- TSV (Tab Separated Values): Text file data with a plurality of fields separated by the tab symbol
- Microsoft Excel/Access or other application files
- Oracle/SQL Server/MySQL or other database files

- IBM i2/LexisNexis CaseMap or other analysis software data files

Some data files are mutually interchangeable in format. Regardless, the first task for an investigator is to ascertain whether the data files he/she has received can be read.

Next the "**Integrity**" of the data that has been received must be checked. Typical checking methods are shown in Table 7–10:

Table 7-10. Checking methods to ascertain data integrity

Checking method	Result
Numeric check	Checks data that must be handled as numerical values does not include characters etc. that cannot be treated numerically
Sequence check	Checks that the target data is arranged in a certain order
Limit check	Checks that the data is within the appropriate range, neither going above the upper limit nor below the lower limit
Format check	Checks that the target data conforms to a specific format
Matching check	To avoid inputting unregistered data, checks that target data has been registered
Logic check	Checks that there is no contradiction with other relevant data With data where, as in a balance sheet, debits and credits must balance, adds up the debits and credits separately and checks that the totals are the same
Duplication check	Checks that there has been no duplicate registration of data that should be unique

●Data Normalization

When data analysis is initiated to aid an investigation, the investigating officer and the administration should agree in advance in regards to what kind of data set should be subjected to what degree of analysis.

In the planning stage, the data should be systematized and arranged within a scientific analytical framework to identify trends that fit the specified investigative scenario. This is called "**Data wrangling**".

By the "**grouping**" and "**summarization**" of data, it is possible to grasp an overview of the entire body of data. This ensures that, if outlying values are found later in the investigation, one can use the overview as a source of reference.

All data must be standardized in order to ensure consistency in analysis. For this purpose, the conversion of some data fields into a standard format may be required. Some typical data formats are shown in Table 7-11:

Table 7-11. Examples of data types

Data types	Distinctive features
Continuous type	Describes a range of numbers (e.g. 1~100). Continuous numbers may include integers, real numbers, dates/times etc.
Category type	Used in character strings where numerical values are not known. Also called uninstantiated data.
Flag type	Used with data comprising pairs of contrasting values such as true/false, yes/no, 0/1, etc., indicating the presence or absence of a characteristic.
Nominal type	Used to describe data having a plurality of different values. Each value is treated as a member of a set, such as “North/South/East/West”.
Ordered type	Used to describe data having a plurality of values with a specific order, such as LOW, NORMAL, HIGH etc.

In some cases, checking the quality of data may lead to the discovery of inconsistencies. The process of addressing such inconsistent data by means such as "deletion" or "complementing" is called **“Data cleansing”**.

Inconsistent data should not be deleted lightly. This is because even where data lies outside the value range, it may have great significance in the process of decision-making. In the handling of data related to cybercrime investigations, investigators must always bear in mind that they are dealing with the value of an illegal transaction. **“Missing Data”** denotes inconsistent data and results from the missing value of a certain item in a certain case. An effective method for resolving this problem is to consider the pattern that led to the deficit. Typical missing data structures are shown in Table 7–12:

Table 7-12. Missing data structures

MCAR (Missing Completely At Random)	Values are randomly missing. Data defective not depending on other data.
MAR (Missing At Random)	Values are missing dependent on observed data.
MNAR (Missing Not At Random)	Values are missing dependent on the missing data itself.

Missing data situations must be dealt with either through the “delete” or “complement” approach. In the case of MCAR, the missing data can be deleted because the loss probability of each data point does not depend on any other data. In contrast, in the cases of MAR or MNAR, there is a risk that executing a deletion may result in an imbalance. These situations need to be dealt with by complementing the missing values.

Typical methods of deleting or complementing are shown below in Table 7-13:

Table 7-13. Methods of deleting or complementing missing data

Missing value handling approach		Details
Deletion	Listwise method	Deletes sample items with missing data
	Pairwise method	By calculating correlation coefficient, distribution, etc., deletes sample items that have missing data in one of two paired variables
Complementing	Unit Imputation method	Complements by adding a predicted value based on the average value and other variables
	Multiple Imputation method	Creates multiple data sets by substituting missing data, carries out an analysis of each data set, and complements missing data by integrating the results
	Full Information Maximum Likelihood method	An assumed likelihood function corresponding to the defective pattern for each sample, using multivariate normal distribution, is obtained by performing a maximum likelihood estimation of the mean and the variance-covariance matrix

"**Outlier Data**" refers to items of inconsistent data that deviate significantly from observation data and values. Investigators must determine the range within which the adopted value falls. This is decided depending on what user is being targeted by measures that reflect the suggestions resulting from the analysis, and on the range of effective analysis required to achieve a result.

Typical approaches for value detection are shown below in Table 7-14.

Table 7-14. Approaches for detecting outlier data

	Overview
Statistical approaches	Data is considered to be generated in accordance with statistical model, and values that do not conform to the model are identified as outlier data
Proximity-based method	Data values that, in comparison with other data, differ significantly from the nearest point are identified as outlier data
Clustering-based method	Data values occupying the smallest cluster when the data is clustered are identified as outlier data

Automation

"Automation" is defined as the use of computers to perform analysis on data of such volume that it cannot be performed manually, using a variety of analytical frameworks and carrying out analysis from different viewpoints.

●Databases

A database is the infrasystem of an analytical framework. The two main categories of databases are relational (RDBS) and non-relational (NoSQL). Non-relational databases can be further broken down into several categories. The most common database types are shown in Table 7-15:

Table 7-15. Database types

Database type	Data storage format	Example
RDBS (Relational Databases)	Tables (rows and columns)	MySQL, PostgreSQL, Oracle
NoSQL Databases		
KVS (Key-Value Store)	Key and value pairs	Redis, DynamoDB
Document-Oriented Databases	Tables (rows and dynamic columns)	MongoDB, CouchDB
Graph Databases	Key and value pairs	Neo4j, OrientDB
Time series databases	Key and value pairs	Druid, eXtremeDB
Wide-Value Stores	Rows and columns	Apache Cassandra, Bigtable

An RDB has a structure which conforms to Atomicity, Consistency, Isolation, and Durability (ACID) characteristics, whereby emphasis is placed on consistency of data. This type of database uses tables with rows and columns to hold data. In contrast, a NoSQL has a structure which conforms to Basically Available, Soft-state, and Eventual Consistency (BASE) characteristics, whereby emphasis is on the usability of the data. As seen in Table 7-15, there are multiple types of NoSQL databases using a variety of methods to hold the data, from key-value pairs and documents to graph structures. In all cases, it is necessary to select a database that matches the processing characteristics required by the system.

●Data Analysis Software

Numerous data analysis software packages are available. Among these are specialist software packages that have been designed for criminal investigations' data analysis use. In many cases, investigators decided to use software that has already been used by their own organization. To assist in cases using new software, the data mining software evaluation criteria developed by Ken Collier is shown in Table 7–16 as a source of reference:

Table 7-16. Data mining software evaluation criteria developed by Ken Collier

Performance	Capability of handling a variety of data sources
Functionality	Inclusion in the program of a variety of capabilities, technical approaches, and methodologies for data mining
Usability	Compatibility with a variety of levels and types of users, without loss of usefulness or functionality
Auxiliary work support	Possibility for user to perform a variety of tasks to support data mining

Microsoft Excel, Google Spreadsheet, and similar programs are said to be the data analysis software products used by the greatest number of organizations. However, these are restricted in terms of the number of data items they can handle and in that, due to their limited function control, they are unable to meet high-level demands for statistical operations such as data blending and cleaning from multiple sources, advanced visualization, and so on.

Programming languages such as "R" and "Python" have come a long way with numerous peer reviewed resources such as books and libraries, and can be a very flexible tool in the arsenal of every investigator. They can help automate repeatable tasks, analyze various data types (from CVSs to PCAP files), apply data mining and machine learning techniques, and visualize and create timelines. Moreover, they can enable the utilization of Application Programming Interfaces (APIs) for tools already deployed in an organization. This can decrease investigation time while allowing for scalability when interacting with a tool that is already deployed. It should be noted that when using telemetry from tools deployed in a network,it is important to ensure CoC and the integrity of data.

Quality Assurance and Control

"**Quality Assurance and Control**" is defined as the process whereby, in relation to an analytical framework, an experienced and skilled person can guarantee the quality of the final output by giving guidance and advice. The criteria for evaluating an analytical framework output entails "**Precision**", "**Reliability**", and "**Practicality**".

Precision is an index that indicates whether the analytical framework' s output has a close relationship with the attributes that have been provided. In the data standardization process carried out within the analytical framework, data cleaning is implemented in respect of inconsistent data. For this reason, when measuring precision it may be necessary to carry out further investigations or studies in respect to inconsistent data.

Reliability shows the performance of an analytical framework with respect to differing data sets. If a general pattern or the same type of output is found to be generated regardless of the data provided, the analytical framework' s evaluation can be judged as highly reliable.

Practicality indicates whether useful information is provided by an analytical framework.

In general, Quality Assurance and Control is closely related to the process of standardizing data.

●Dissemination of plans for quality maintenance

In the process of Quality Assurance and Control, the target level and order of priorities should be determined in advance. Frequently used information and information that has a major impact on criminal investigations should be given a high level of priority. Investigators should also consider removing information that they do not intend to use.

Consistent maintenance of data is not solely achieved by the investigators in charge of analysis. It should be achieved by all investigators involved in an investigation. It is therefore indispensable to carry out regular training around the correct policies and procedures for managing data.

Data is always changing. It is necessary to conduct regular reviews of quality management processes in response to changes in data.

●Monitoring for the purpose of quality maintenance

Data quality can deteriorate quickly if not properly managed. Regular monitoring, including weeding out data, should be carried out to prevent the dissemination of out-of-date and mistaken information. For the purpose of maintaining consistent data, it is necessary to pre-establish a system of automated data management with reports, dashboards, and so on, which anyone can check when necessary.

Interpretation of Results

Interpretation of Results deals with definitions of "Threat Profile", "Attribution Profile", and Impact Analysis. In criminal investigations, not all found evidence is conclusive. However, by building associations between limited items of evidence, it is possible to find context which in turn creates a decision-making cycle based on the information.

Threat Profile

"**Threat Profile**" is defined as a crime scenario, involved "threat actors", and information about the threat.

By analyzing an occurring threat and recording the "Actor Class" as categorized in Table 7-17, the "Actor Motivations" as shown in Table 7-18, and the "Actor Sophistication" as shown in Table 7-19, cybercrime investigators can describe the interaction between these conditions. This helps investigators give police management an understanding of the crime situation, and can be used to analyze police activity.

It is worth noting that there is a need for future research to expand on these items and develop more detail by creating subcategories.

Table 7-17. Actor Classes

Actor Classes
Competitors/Espionage
Disgruntled Customer/User
Hacktivists (Criminals who engage in hacking activities in pursuit of social/political goals)
Insiders
Organized Crime
Script Kiddies (Criminals who cause harm to 3rd parties for their own entertainment)
State-Sponsored (APTs)
Terrorists

Table 7-18. Actor Motivations

Actor Motivations	Subcategory
Financial or Economic	
Ideological	Corruption
	Anti-Establishment
	Environmental
	Ethnic/Nationalist
	Information Freedom
	Religious
	Human Rights
Industrial	
Military	
Opportunistic	
Political	
Prestige	

Table 7-19. Actor Sophistication

Actor Sophistication
Innovator
Expert
Practitioner
Novice
Aspirant

Attribution Profiles

"**Attribution Profiles**" consist of information about criminals or the preliminary groups from which they are recruited. Many risks are concealed within business relationships and human networks. It is therefore important to expose these risks by analyzing and recording attribution profiles and promoting an understanding of hidden threats.

Preliminary groups that should be recorded include high-risk individuals and groups, including their partners and families. Furthermore, from the perspective of "**AML (Anti-Money Laundering)**" and "**CFT (Countering the Financing of Terrorism)**", "**PEP (Politically Exposed Persons)**" should also be monitored **(monitoring)**. Table 7-20 shows highly private attribute information that can be obtained from very reliable sources.

It is also important to compile findings obtained from the aggregation of information on public record. Where there is no preliminary group criminal history, the use of public information is a powerful clue in an investigation.

Table 7-20. Attribution Profiles

Attribution Profiles
Photo
Last Name
First Name
Gender
Marital Status
Alternative Spelling(s)
Alias
Native Character Name(s)
Workplace
Title
Date of Birth
Place of Birth
Country of Birth
Nationality
Current Address
Telephone Number
Email Address
Social Media Account(s)
Passport No.
Driving License No. (and numbers pertaining to any other official personal documentation)

Impact Analysis

"**Impact Analysis**" consists of information about victims and the scope of cybercrime as indicated by the number of systems, users, and so on that were accessed or used without authorization. It is critical to document impact analysis in a per-system, per-user, or related standard format. This enables investigators to compare similar details quickly. The use of a case management system can assist with relevant analytics.

Artifacts should be recorded according to the dates of their origin or change to describe the incident timeline for impact analysis, as shown in Table 7-21Response recommendations for emergency and remedial actions should be documented in accordance with organizational policy and jurisdictional guidance.

Table 7-21. Impact Analysis

Impact Analysis
Affected System(s)
Affected User(s)
Affected Information
Incident Timeline Artifacts
Response Recommendations
(a) Emergency Actions
(b) Remedial Actions

Cryptocurrencies and Blockchain Forensic Capabilities

One final topic worth discussing is the recent rise in the use of cryptocurrencies to obfuscate criminal transactions. Given the trendlines, the use of in-depth digital forensics and analytical techniques has become increasingly critical in identifying key artifacts, transaction histories, and indicators of illicit activities, particularly in scenarios that require formal presentation to courts by law enforcement for disruption, asset forfeiture, and seizure. Digital forensics and analytics play a critical role in unraveling seemingly complex transactions involving cryptocurrencies, often utilizing bespoke, open-source, and industry-recognized tools and methodologies to trace transactions, identify ownership, and establish patterns of behavior. For example, the exploitation of the Ronin Bridge --an app for transferring Ethereum Blockchain and non-fungible tokens (NFTs) between Ethereum and the Ronin chain -- led to a $625M heist of Ethereum (ETH) and USDC tokens in 2022[253].

One of the core challenges in investigating matters involving digital assets is the pseudonymous nature of cryptocurrency transactions. Identifying ownership of digital wallets can be challenging, but blockchain forensic software capabilities are evolving to include additional insights to contextualize what can be observed on-chain.

Law enforcement and cybercrime investigators are uniquely positioned to employ sophisticated techniques to attribute transactions to specific entities and individuals. This includes analyzing blockchain data, tracking wallet addresses, identifying key behavioral patterns, and utilizing additional Open-Source Intelligence Tools (OSINT), including deep and dark web resources collected from reputable companies to help identify actors behind the fraud, theft, or extortion event. The integration of advanced analytics ensures a comprehensive understanding of the digital trail left by individuals involved in questionable activities.

[253] https://www.fraud-magazine.com/article.aspx?id=4295019793

Chapter 7: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts) and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

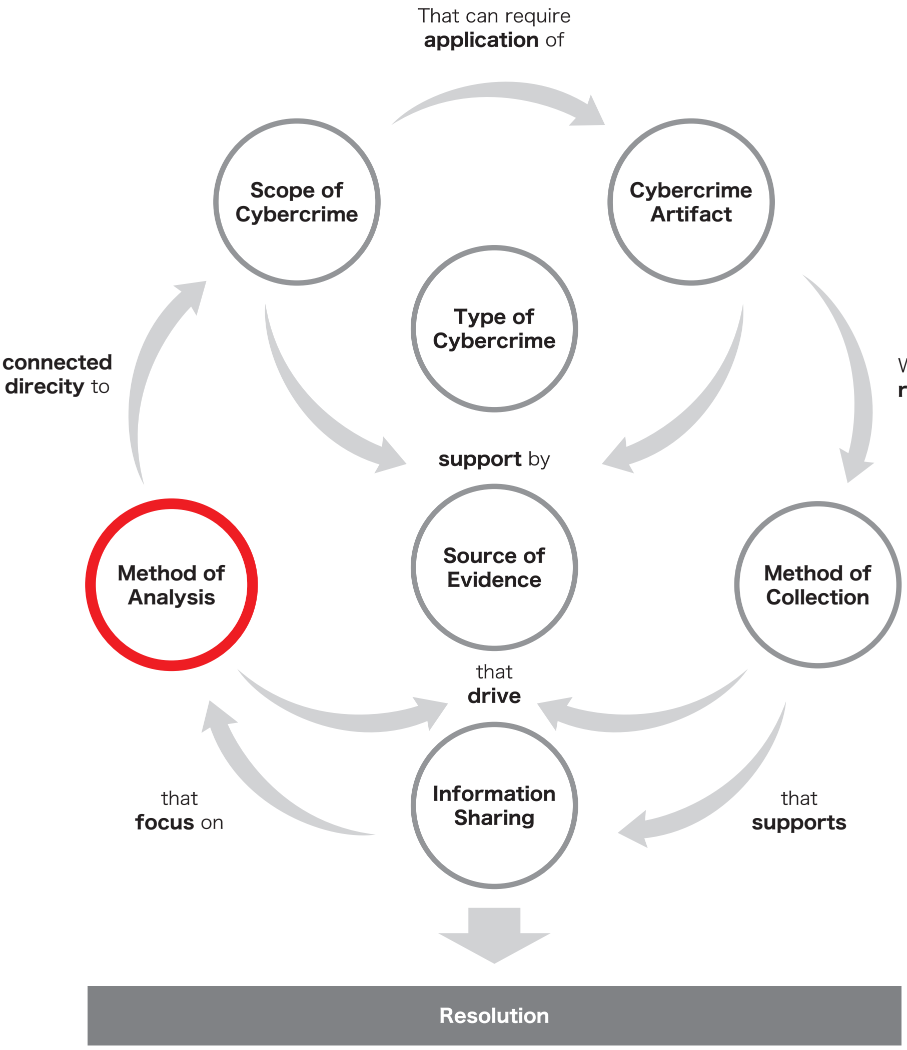


Figure 7-6. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 7-7. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 7-8. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

<legend>
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should have a procedural understanding of jurisdictional guidance concerning evidence analysis and interpretation. They should have strategic responsibility for defining and managing related policies.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. Intelligence staff should have a procedural understanding of evidence analysis methods (and limitations), and tactical knowledge of how to process evidence.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigative staff should have a procedural understanding of evidence analysis and reporting methods (and limitations), and tactical knowledge of how to process evidence.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well as methods and restrictions concerning analysis of evidence to inform policy makers.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The type of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when.

Support – require tactical and procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 7: Review

1. How should evidence be aggregated and analyzed for the purpose of cybercrime evidence analysis?

   Answer: Aggregated by ETL methods into a database for analysis

   Examples: Log standardization and an EDM that defines types, relationships, and entities

2. How should efficient data management and analysis frameworks be defined?

   Answer: Scalable and iterative with quality control checks

   Examples: QC tests on data quality, query review by QA analysts, results review by second party

3. How should analysis results be recorded and associated with the scope of the cybercrime?

   Answer: In a case management system that includes a notification/sharing feature

   Examples: Case 1 at date XX relates to Case 4 at date YY, IOCs were ZZ and shared

4. How should impact analyses related to "threats," "activities," and "threat actors" be interpreted?

   Answer: According to scope of victims/systems and objectives of the cybercrime, not only identity

   Examples: What was done, when, how, and where it affected how many people/systems is more important than who specifically performed it. Why is the ultimate evidence that analysis will reveal to assist investigators in defining the (scope and purpose) of the crime, so that means/motive/objectives can be determined to identify suspects.

Case Study 7: Attempted Server Breach

- **Crime**: Unauthorized computer access
- **Suspect(s)**: Unknown
- **Means**: Malware, Living off the Land
- **Motive**: Unknown- potential economic interests
- **Opportunity**: Access to leaked privileged user credentials, unsecured server password storage

A law firm outsourcing its security monitoring to a third party managed security service provider receives a security alert. The security provider notifies the firm regarding a possible indicator of compromise related to a service account being used to login via RDP on one of the firm' s backup servers. Available logs confirm this was a failed login, but the type of activity, origin, and time are not in line with the baseline of the account. After internal escalations, it is confirmed that this is not expected and the credentials- as well as the server- are considered compromised. Due to the sensitive customer data the firm stores on the server, a possible major incident is declared and the firm' s predefined incident response plan is followed. As a result, the involved entities are isolated and remediated as needed and a third party investigator is assigned to the case. At this point, the only known details are the service account used for the RDP connection, the source device of the connection, and the target server. To collect more data to inform the investigation, the investigator performs the following tasks:

- A proprietary threat intelligence tool is utilized to search for external intelligence regarding the law firm. This results in the identification of multiple leaked credentials for users in the firm. However, it is not clear which of these credentials are for internal applications and which are for external services. The credentials list is subsequently filtered by comparing the collected leaked credentials to the password policy of the firm.
- An EDR capability-already in place within the firm' s estate- is leveraged to collect events related to persistence mechanisms and processes, network, and file activity from all available devices. This produces a dataset of a considerable size, which if efficiently analyzed might provide valuable IOCs for the incident and a first view on the scope of the compromise.

Multiple analysis methods are then used on the collected dataset. Domains, IPs, and hashes are first cross-referenced with known IOCs to form threat intelligence. Statistical analysis is then performed on events to identify outliers that are present only on a small number of devices. Since the investigator has access to a large percentage of the company' s estate while performing the investigation, the creation of a baseline for different types of assets (e.g. servers vs end user devices) is enabled, as is a more efficient identification of uncommon events.

The analysis produces a small number of events of interest which need to be manually reviewed. Through manual review, the investigator uncovers the following confirmed IOCs:

- An unknown executable "fox.exe" in the "C:\Temp" directory of some EUC assets and one server asset.

- A Windows service through which the fox.exe executable persists on the devices.
- A list of IPs with which the executable has initiated connections.

At this point, the investigator provides the information uncovered to the firm and the third party security provider. This ensures that:

- The compromised devices are isolated to limit the damage.
- Forensically sound collections of the hard disk and memory are performed for compromised devices.
- The IOCs are used to strengthen the firm's security controls (e.g. block IPs) as well as enhance their monitoring.

From the collected evidence, the investigator then extracts three variations of the "fox.exe" executable and hands them off to another team for analysis. While that analysis is taking place, the investigator analyzes the collected disk images and memory samples and correlates them with the previously found leaked credentials. One of the compromised devices is identified as the primary work device for a user whose credentials were recently leaked on the Dark Web. The investigator requests all authentication activity for this user as well as the primary users of all other EUC devices. This results in the identification of a login from the user two days after the leaked credentials were advertised, from an IP that does not match the user' s baseline.

These findings indicate that this device might have been patient zero and that attackers pivoted to the rest of the devices through other methods. Moreover, an analysis of the disk shows a Window profile for the compromised user on the other EUC devices, but not the servers. This indicates that patient zero' s user credentials do not allow for lateral movement to non-EUC devices. An analysis of various Windows events on the devices shows unexpected RDP activity and logins using the compromised user' s account. This confirms how the attackers moved from one EUC device to another, but not how they pivoted to the servers.

Furthermore, an analysis of the executable concludes that it is a type of modular malware that allows remote execution of various commands, including the loading of other tools in memory and the use of various evasion mechanisms such as injecting itself in legitimate processes. Using the collected memory dumps, the investigator identifies several injected processes and extracts the injected code. Further analysis produces a list of known malicious tools that could be used to perform credential access and discovery activities. Focusing on the compromised servers, the investigator identifies one domain admin account that the malicious processes were running under. As before, the new findings are provided to the firm for further containment actions.

It is not clear through the evidence how the privileged account was compromised. However, through an analysis of files on one of the servers, the investigator finds a plaintext file containing the password of the original service account used to attempt to login via RDP to one of the firm' s backup servers. Further communication with the firm' s IT team and a review of the password change logs reveals that the service account password was recently (prior to the malicious failed login) changed, and thus the plaintext file contained the previous password. Finally, based on the identified TTPs and IOCs (IPs, hashes, filenames, and compromised accounts), no other devices appear to have been compromised and the incident appears to have been contained. The investigator follows expected procedures to produce the proper documentation and reports.

Chapter 8

Resolution

Introduction

Understanding what makes for an effective response to a cybercrime means asking not only “how” an incident is resolved, but also “who” should be involved in the resolution and “when” they should become involved. Resolution of cybercrimes involves organizational efforts to assess, investigate, understand, and remediate – both technically and procedurally. An effective resolution is not simply a matter of replacing a hacked system. It starts well before an incident occurs, with an assessment of what information assets the organization has to protect, what risks it faces that shape how it should invest time and resources to defend itself, and what planning and testing is necessary to improve the organization’ s posture to prevent or respond to cybercrimes. Thereafter, it includes the activities in the “normal course of business” that should be defended through awareness and preventative and investigative means.

To understand the normal course of business from a cyber security perspective means conducting a business impact assessment that gauges the impacts of disruptions of different types. This assessment should include the identification of critical systems, processes, and data, as well as the potential financial, reputational, and operational consequences of a cyber attack. By understanding the importance of these assets and their potential vulnerabilities (and associated impacts), organizations can better prioritize their resources and efforts to protect them.

The key components of a cybersecurity business impact assessment (BIA) include:

1. **Identification of Critical Assets**: This involves identifying and prioritizing the organization's information assets to understand their importance in core business functions[254].
2. **Impact Analysis**: The BIA focuses on evaluating the potential effects of an interruption to critical business operations, such as delayed sales, increased expenses, regulatory fines, and customer dissatisfaction[255].
3. **Risk Analysis and Management**: The BIA serves as a foundation for risk analysis and ongoing risk management, helping organizations allocate resources effectively and implement appropriate security measures[256].
4. **Recovery Strategies and Contingency Plans**: This involves developing resiliency strategies, creating contingency plans, and mitigating disruptive events with measures such as backup plans, contingencies, and recovery protocols[257].
5. **Resource Interdependencies**: Understanding resource interdependencies and the flow of sensitive data is crucial for assessing the impact of an incident on operations and establishing recovery time requirements[258].

By considering these components, organizations can better understand the potential impact of a

[254] https://clearwatersecurity.com/blog/business-impact-analysis-a-critical-process-for-to-improve-resiliency-in-wake-of-a-cyber-attack/

[255] https://www.techtarget.com/searchstorage/definition/business-impact-analysis

[256] https://www.cybersaint.io/blog/cybersecurity-risk-management-framework-key-components

[257] https://www.cm-alliance.com/cybersecurity-blog/the-importance-of-business-impact-analysis-in-cybersecurity

[258] https://coreitx.com/blogs/8-elements-of-a-business-impact-analysis-bia-for-compliance

cyber attack and develop strategies to minimize disruptions and recover effectively.

Once the BIA is complete, organizations need to implement appropriate defensive measures to safeguard their operations against the “ABC’ s” (Attack, Breach and Compromise) they face from cyber threat actors.

In addition to preventive measures, organizations need to have a thorough incident response plan in place. This includes having a dedicated team responsible for detecting and responding to cyber attacks, as well as clearly defined steps for containing and mitigating the impact of an attack. It is crucial that this plan is regularly tested and updated to ensure its effectiveness.

Furthermore, with the rise of cloud computing and the increasing use of third-party vendors, it is important for organizations to not only secure their own networks but also those of their partners and suppliers. This involves conducting due diligence on the security practices of these entities, implementing strong contractual agreements, and regularly monitoring their systems for any signs of compromise.

Another aspect of effective cybersecurity is staying informed about the latest threats and vulnerabilities. This can be achieved by following industry news and advancements, attending conferences and training sessions, and joining online communities of cybersecurity professionals.

Additionally, employees play a crucial role in maintaining the security of an organization's network and preventing attacks, mitigating breaches, and disrupting and investigating compromises that may originate from inside or outside the organization.. It is important for companies to provide regular training and education on safe computing practices such as how to identify phishing emails, how to create strong passwords, and- most importantly- when and how to report when something doesn’ t seem right or they might have made a mistake. Organizations should also implement strict access control measures to ensure that only authorized personnel have access to sensitive information.

This chapter will describe the roles, assignments, actions, and procedures used to investigate and respond to cybercrimes. It will also explain how the scope, artifacts, sources, and evidence of cybercrimes relate to the process of resolving incidents according to organizational or jurisdictional policies. Because different cybercrimes vary in their impact, so too will they require different investigative and resolution techniques.

This chapter will additionally provide investigators with a suggested framework for responding to a cyber incident and remediating vulnerabilities according to best practices and liability-related considerations found in many jurisdictions. This will also assist organizational managers in defining associated policies, systems, and procedures for defense and protection.

It is important to note that the legal and regulatory implications of many of the issues and actions discussed in this chapter vary by jurisdiction. The purpose of this chapter is not to provide legal advice and should not be relied on as such. Rather, it is intended to provide an overview of the legal and practical considerations that investigators should take into account when applying the facts and locally applicable law to cyber incident response.

At the conclusion of this chapter, readers will have an understanding of:

- How should a cybercrime investigation and resolution function be organized?
- What are the components of a business impact assessment?
- What are the ABC’ s of cyber security?

- What methods of communication, and with what authority, should be established for phases of cyber investigations and resolution?
- Who should be involved in cybercrime investigation and resolution program functions, and when?
- What tools, personnel, and procedures should be aligned for resolution?

Topic in Resolution

Figure 8-1 displays topic categories in the “Resolution” knowledge domain.

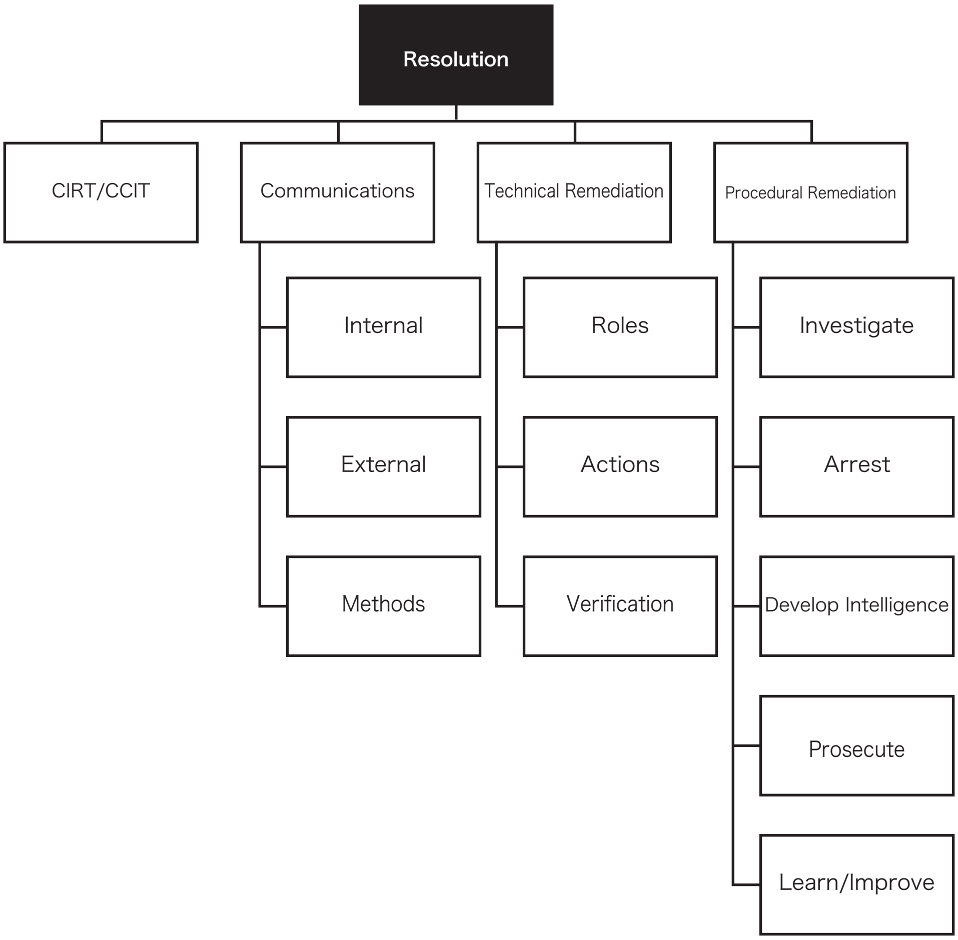


Figure 8-1. Topic Categories in the “Resolution” knowledge domain

What is Resolution?

Resolution of a cybercrime “incident” refers to several things. An organization’ s cyber incident response must extend beyond its technological reaction and encompass management of the increased risk of liability associated with an incident. Resolution is about bridging the activities of an organization, with its varied and distributed resources (and different mission objectives), with the activities of Law Enforcement/Intelligence organizations who have their own resources and objectives.

We are well past the time when a major cyber incident elicited shock or surprise from the public. The onslaught of large-scale breaches in recent years has caused the public, regulators, the media, and plaintiffs’ attorneys to demand cybersecurity awareness and preventative action on the part of company management.

Put simply, we are now in the liability phase or, perhaps more broadly, the “accountability phase” of preventing and responding to cyber incidents. For law enforcement investigators and intelligence/counter-intelligence operators, this new reality has particular implications around the likelihood that private entities will come forward to report cybercrimes, as well as the degree to which they will provide access and evidence to investigators.

Resolution addresses more than technical response. Instead, it considers important issues of communications and technical/procedural remediations available to an organization or victim. Sometimes those remediations are according to organizational policies and other times they are governed by applicable laws that may involve legal evidence collection and the prosecution of perpetrators. Such is the nature of crime, whether traditional or cyber.

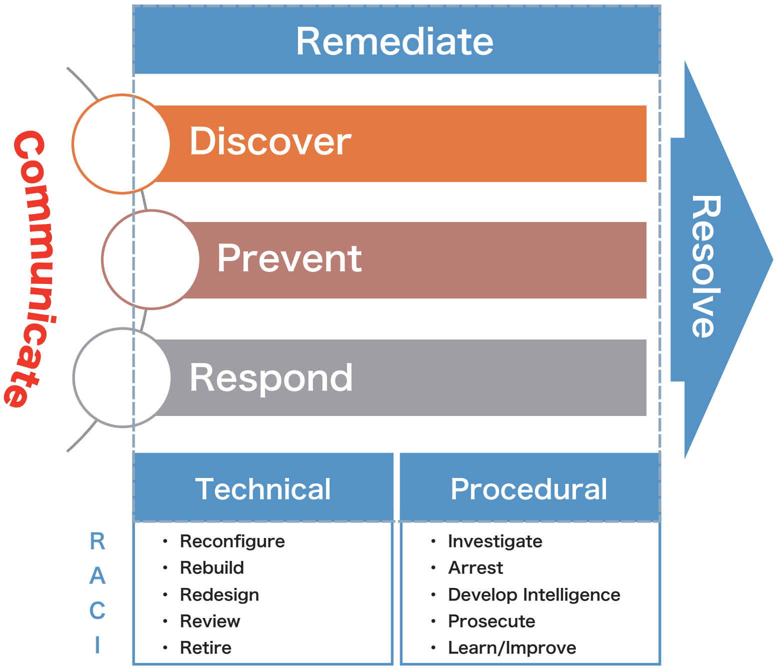


Figure 8-2. Cybercrime Resolution Model

Incident Investigation and Response Organization

Cyber security incident response teams (CSIRT) in organizations have evolved to address cybersecurity needs of businesses such as continuity of operations, business functional security needs, and information governance and protection. The CSIRT model comes from Critical Incident Response Teams (CIRT) and Computer Emergency Response Teams (CERT), concepts that have existed much longer than the concept of “cyber”. CIRTs were primarily originated in Law Enforcement, driven by local responders’ needs to organize talents, skills, staff, and equipment – as well as associated jurisdictional policy and permissions – to enable quick response to emergencies or other incidents as they were reported. Over time, the concept was adopted by private industry and other public sector organizations to describe similar functions. CERTs were one such evolution of the CIRT concept that emerged in 1998 after a large-scale computer virus attacked computers across the Internet- hence the first CERT (Carnegie Mellon University’s Computer Emergency Response Team – Coordination Center[259]) was born. Over time, CERTs- often renamed as CSIRTs or CIRTs (as “Cyber” Incident Response Team)- have been adopted in business continuity and information security planning and governance by both public and private sector organizations. CCIT (fcybercrime investigation team) is also sometimes used.

Establishing documented policies and procedures for investigating, collecting evidence, and reporting is critical to success. Management will look to CIRTs to fully investigate an incident and minimize the exfiltration of data. They will expect CIRTs to determine how the attackers gained access, how and where they moved laterally within the network, what data was sought and collected, where data was staged for exfiltration, and what data was actually removed from the premises and by which route. CIRTs will identify security weaknesses that were exploited by the intruders, which may range from zero-day malware and unpatched systems to phishing and social engineering of employees and vendors who had access to the network. CIRTs are expected to identify other compromised systems and often image those machines for evidentiary purposes, and then rebuild and harden them through reconfiguration before they are restored to the network.

Management’s support of and reliance on its CIRT is essential. The business’ reputation is protected by having a capable and efficient CIRT. Organizations possess and store data from other companies, vendors, sub-contractors, and the government in order to conduct their daily business operations. Consumer companies such as Target and Amazon are entrusted with the credit card data and PII of their customers. If consumer confidence is lost in the company’s ability to protect such data, people will discontinue their business dealings with the company. Likewise, in the government/defense industry, many contractors work with other companies in research and development projects for product manufacturing and maintain extensive supply chain relations. All of these relationships have contractual obligations and can expand the company’s liability in the event of a data breach. While a company may survive the initial cyber attack, a lot more depends on whether their customers maintain confidence that the organization is still a trusted brand.

Management must be able to prove that its IT infrastructure is in compliance with legal requirements and that their CIRT will continually monitor, investigate, and work on the continuous

[259] https://en.wikipedia.org/wiki/Computer_emergency_response_team

improvement of security to protect everyone' s data. To achieve these objectives, an organization of responsible and accountable internal and external resources must be defined, and supported by tools, staff, and procedures.

Communications

When a cybercrime occurs, the first and foremost consideration for an organization is communication. Many organizations focus their efforts on discovering, preventing, or responding to incidents, but communication is required across all of these functions. Who should communicate, with whom (inside and outside of an organization), what information they should share, why, and how the information should be communicated are primary concerns.

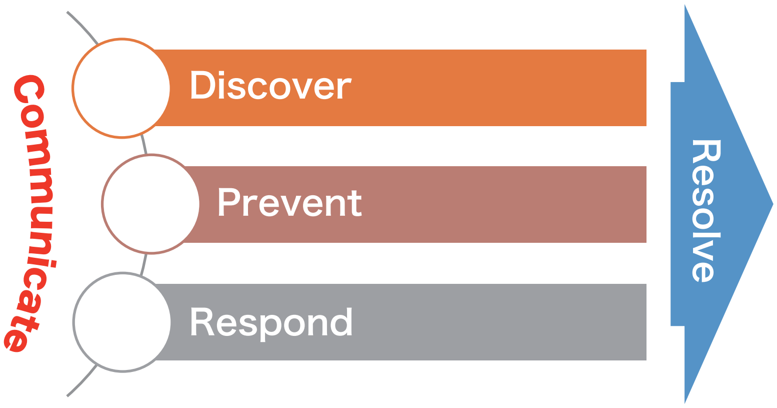


Figure 8-3. Communicate to Resolve

Internal

CIRT processes should establish lines of communication, the requisite information that each line provides to a target consumer (including its format, content, timing, and the delivery mechanism), and who should deliver the communication. This is sometimes referred to as a "Red Book" notification process. Law enforcement and other investigators should define similar processes for notification procedures and communications with victims.

Internal notifications typically involve the following internal organizational consumers, organized according to the methods that relate to their notification or involvement in the process:

Table 8-1. Internal Communications

Method of Notice	Consumers
Technical Alerting	Investigators
Case Management	Investigators, CIRT, Business Functions (Risk Management, General Counsel, IT/IS, etc.)
Red Book	Business Functions, Executive Staff
Sharing Portal(s)	Business Functions (IT/IS)
STIX/TAXII/IOC Sources	Business Functions (IT/IS)
Audit Reports[260]	CIRT, Business Functions (Affected Department Heads, Audit and Governance)

External

Organizations have several consumers to notify and communicate with throughout an incident resolution process. Besides internal consumers there also are interested external parties, some of which are "second parties" with interests in the organization (such as outside counsel and shareholders) and some of which are "third parties" who may be impacted by incidents that affect the organization (such as the public, industry, law enforcement, and insurance companies). Sometimes the lines between second and third parties are not obvious. However, the essential issue is that in addition to the internal consumers, CIRTs have many external consumers that should be addressed in their red book plans and processes.

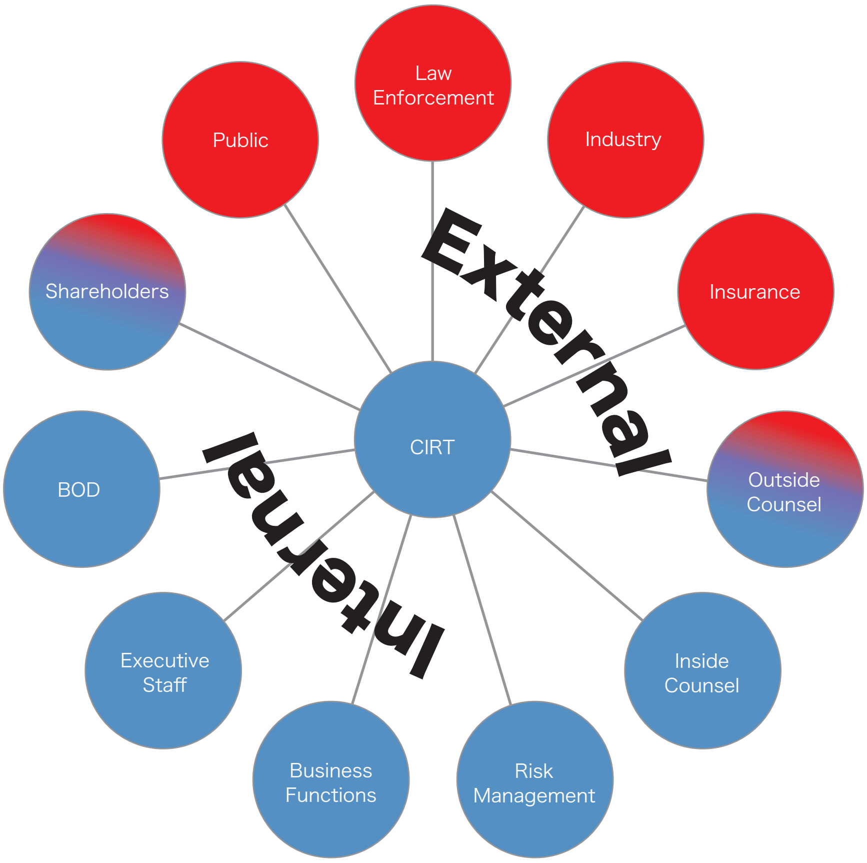


Figure 8-4. CIRT Information Sharing

[260] Note that "Audit Reports" in this context include "After Action Reports" as well as periodic performance improvement testing and reporting.

In the ideal situation, a cybercrime investigator is not meeting a victim for the first time when a major incident occurs. In recent years, investigative agencies such as the FBI and the U.S. Secret Service have made tremendous efforts to reach out to companies with guidance (and to further inform individual computer users) before an incident occurs. Establishing a relationship prior to a breach allows an investigative agency to not only explain the evolving threats associated with cybercrime, but also to streamline potential responses and provide some measure of familiarity and trust. Public-private data sharing centers such as the U.S. National Cyber Forensics & Training Alliance (NCFTA)[261], the Japan Cybercrime Control Center (JC3)[262], and the National Cyber Security Centre (NCSC)[263] in the UK represent important platforms for collaboration such as exchanging threat information, building working relationships, and raising the level of preparation by both companies and governments.

Public companies and even "sister agencies/departments" within government are cautious about the extent of a relationship with law enforcement. Historically, most of their interactions with law enforcement have been on the basis of served subpoenas or warrants, and not positive relationship-building efforts to align talents and interests. Victims are often very hesitant to report cybercrimes to law enforcement. They fear a range of consequences in doing so including public disclosure and embarrassment, loss of customer and client trust, regulatory sanctions, liability for failure to safeguard third-party information, and ultimately loss of control over the situation. Their relationships with investigators have also been hampered by variations in the levels of technical capabilities and understanding of cybercrime across different law enforcement agencies. When law enforcement consistently invests the time and effort to forge relationships not only with companys' in-house technical teams but also with leadership, a cooperative and productive relationship can emerge. Both public (including law enforcement) and private organizations are slowly beginning to recognize that each has limited resources and visibility into intelligence and investigation results to address cybercrimes.

Furthermore, a victim that is familiar both with the general law enforcement team and personnel responding to a situation is much more likely to cooperate proactively in the investigation. If nothing else, the victim will know whom to call when a major incident occurs rather than spending precious time struggling to find the correct first responder. In the absence of significant cooperation from a corporate victim, law enforcement is typically forced to resort to using compulsory legal processes to force the victim to divulge information. This can directly impede investigators' ability to collect (and understand) important evidence, and can lead to mistakes by organizations who might attempt ineffective technical resolutions.

In many cases, a victim of cybercrime does not have a choice about whether to inform law enforcement. The average time it takes for a victim to discover an intruder in their network is many months, so stolen data often appears on the black market or in another location where investigators, security researchers, or the media learn about the incident first. This leads to a directed collection of evidence. In many other instances, the company will have mandatory breach reporting and/or victim notification obligations that require it to disclose the incident; for example, the European Union's General Data Protection Regulation (GDPR)[264] requires that a loss of personal data must be reported to the appropriate regulator within 72 hours of discovery.

[261] https://www.ncfta.net/

[262] https://www.jc3.or.jp/

[263] https://www.ncsc.gov.uk/

[264] https://gdpr.eu/

Who to notify, with what information, and what to expect in return are all important considerations for an organization (or individual) that is a victim of cybercrime. Local police forces in most regions of the world typically respond only to physical crimes such as breaking and entering, the theft of goods or property, and violence against persons. Federal agencies are tasked with cybercrimes, but how to reach them with information to assist with resolution remains a common question.

For example, in the USA the FBI is the primary point of cybercrime contact and response. In other countries, it is not as clear. Many countries do not have trained resources or federal structures to address geography-spanning issues such as cybercrime and instead rely upon INTERPOL or EUROPOL. Both international police agencies (aggregates) have cybercrime investigation and response coordination capabilities, but the enforcement of relevant laws and related prosecutions are performed by domestic courts in the countries where victims are physically located or where perpetrators are arrested.

Required disclosures can also arise when the company has contractually bound itself to do so, whether to an insurer, investor, or counterparty to a business transaction, although none of those situations necessarily involve broader public disclosure. Where none of these situations apply, the organization has the luxury of making its own decision regarding whether to report a cybercrime and many still decline to do so. This is largely because of the liability concerns associated with making an incident public, fueled in part by the conflict between turning information over to regulators (hence waiving legal privilege and, as may be available under U.S. law, "attorney work product" protections) and having it used against the company in regulatory proceedings and civil lawsuits.

While liability concerns remain a significant issue, there are potential benefits of reporting a crime that should be taken into consideration and weighed against the risks of doing so. The most obvious benefit of involving law enforcement is added capabilities and institutional knowledge that could significantly assist in determining what happened and who was behind the crime. It's true that technical capabilities have become more available in markets like the United States where there are now many strong forensic resources with excellent skills and significant experience investigating cybercrime methods and tools. These resources do not, however, have the ability to compel the production of evidence and leverage law enforcement relationships around the world.

Another benefit of involving law enforcement, especially immediately after discovering an incident, is that it gives the company the ability to claim it has acted responsibly to regulators, customers, insurers, the media, and others. If a breach becomes public later on in an investigation, it may result in significant embarrassment for the organization. In particular, if a breach affects third parties proactively involving law enforcement can be worth the potential risks of disclosing the related incident(s).

Law enforcement should take advantage of the opportunity to build working relationships with victim companies by conducting periodic (general and sector) threat briefings and updates. This approach enables law enforcement and victim organizations to work together more effectively during an investigation.

Certain information should be protected by an organization. The disclosure of systemic/technical alerts, case management information, and red book information is inappropriate as it represents "work product" that analysts and organizational functions use as artifacts in the process of determining risks and related responses. These artifacts are also used by investigators and prosecutors and should be treated as privileged.

Table 8-2. External Communications

Method of Notice	Consumers
Technical Alerting	Law Enforcement (as requested)
Case Management	Law Enforcement (as requested)
Red Book	Law Enforcement (as requested)
Sharing Portal(s)	Law Enforcement, Industry Sources, Media, Public
STIX/TAXII/IOC Sources	Law Enforcement, Industry Sources, Other Sources
Audit Reports[265]	Shareholders, Media, Public

Methods

Although this chapter focuses on the resolution of cyber incidents, it is important to note that an organization' s ability to manage cyber risks and effectively respond to a breach is determined to a large extent by its preparation ahead of time. Effective preparation has several essential components including:

- Mapping the organization' s information assets (systems and staff) by determining the categories of data the organization has to protect, where they are stored, and how they are secured. Unfortunately, many IT departments fail to understand the link between assets such as servers, cloud containers, or applications and essential business processes; establishing this alignment is a key part of risk management and effective preparation. This process includes mapping the organization' s physical and logical information processing assets (servers, laptops, cloud containers, etc.) with their connectivity (network layouts) and "service owners" . This information is often contained within an organization' s IT service catalog or configuration management database (CMDB) but should be reviewed from a cybersecurity perspective, as it is a high value target for threat actors and should be appropriately secured.
- Creating a multilayered technical security plan that provides increased protections for the organization' s most valuable information assets, while perhaps allowing less restrictive and therefore faster access to certain categories of routine information. Modern cyber attacks are often subtle and may make use of a wide variety of tactics, techniques, and procedures (TTPs). As such, a cyber mature organization should have effective monitoring to understand what 'normal' activity looks like so Security Operations and incident response teams (IRTs) can investigate deviations from the baseline.
- Developing an incident response plan (IRP) that includes procedures that determine how cyber incidents will be triaged and handled.
- Establishing an incident response team (IRT), including representatives across several areas of expertise in the organization, to implement the IRP on an ongoing basis.
- Practicing the IRP through periodic drills in which the IRT and senior officials of the organization test their response to a simulated breach. One of the findings across many cyber attacks in recent years is that drilling the technical and business members of an Incident Response Team (IRT) enhances their efficiency when dealing with actual threats. Though it is unlikely that an

[265] Note that "Audit Reports" in this context include "After Action Reports" as well as periodic performance improvement testing and reporting.

actual attack will be exactly the same as a drill, the "muscle memory" and confidence to respond can make a significant difference.

- Training employees about cybersecurity and cybercrime threats and their responsibilities around managing passwords, handling suspicious emails, and other important safeguards. It is vital that employees are also trained in how to respond to a suspected or actual cyber attack: for instance, who to immediately contact if they have concerns. Many cyber professionals refer to the earliest stage of an incident as "the golden hour" (taken from healthcare), the critical period in which an organization can significantly improve its chances of fighting off an emerging cyber attack before attackers gain persistence and administrative privileges.

Organizations should invest the time and resources to put these pieces in place before they are faced with a significant cyber incident. Indeed, in numerous industries, many of these actions are becoming regulatory requirements or are mandated by cyber insurance policies. CIRT owners should develop associated communications plans that include methods as well as internal and external targets of communication. Targets should receive specific information including what is important, relevant schedules, relevant levels of detail, and how the information should be classified for handling. In this context, classification of information refers to sensitivity, priority, and governing policies or laws which will be discussed in more detail in Chapter 9.

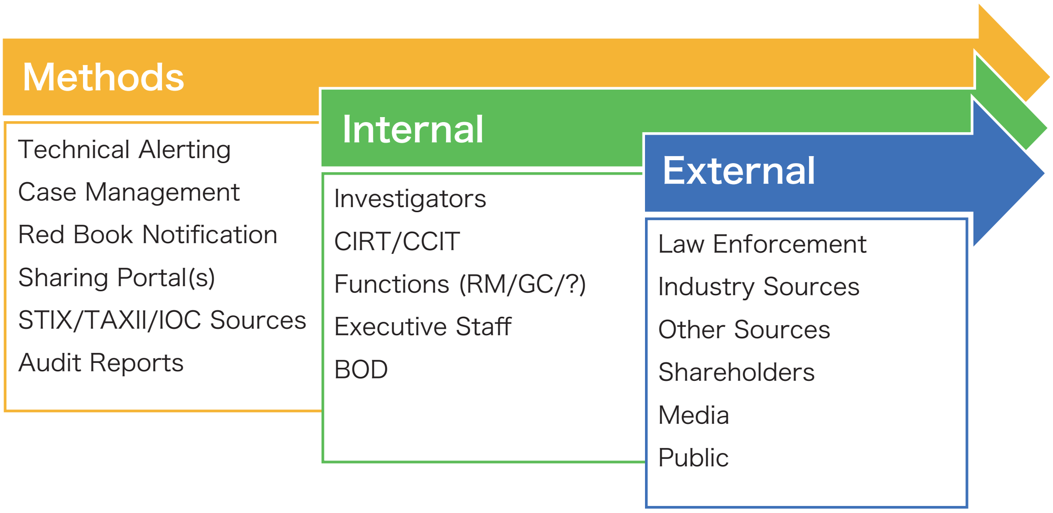


Figure 8-5. Communications Plan

Technical Remediation

Cyber incident remediation is much more than simply the technical actions IT takes to remove a compromised computer from service, reimage it, and return it to service. Rather, technical remediation involves root cause analysis and an investigation of the environment (network and users) that the computer is used in, its relation to other computers and servers/services, and the nature of the cybercrime being investigated. For example, sometimes it is necessary (or investigators are directed) to monitor the compromised host to gain valuable intelligence, and simply rebuilding the computer would impede that activity.

Role Assignments

An unfortunate response by many IT and IS personnel is to remove a “threat” (indicating a simple misperception which is too often reinforced and broadcasted by popular media due to vendor efforts to declare tools such as malware are “threats” without regard to whether, how, or in what context they were used) rather than follow a procedure that would describe the issue, associate it to a business risk by category and type, and notify appropriate consumers of the information through technical alerting or (ideally) a case management system. An organization that practices strong CIRT principles will have methods (and tools) to alert investigators or case management analysts, who then determine whether escalation should occur. If escalation should occur, the associated business function(s) should be made aware of the potential or documented risks as available and should be consulted concerning business impacts with regard to remediation, according to organizational policy and related legal/regulatory requirements.

These criteria for decision-making in cybercrime (or indeed any incident) remediation refer to a common organizational planning and risk management acronym known as “RACI”. Table 8-3 below provides more detail:

Table 8-3. RACI Criteria

Role	Meaning	Example
Responsible	Who is responsible for a decision?	The CIRT leader will escalate critical incidents that potentially threaten the continuity of business/functions to executive staff.
Accountable	Who is accountable for the activity?	The investigator of an incident will ensure appropriate chain of custody is created for evidence in accordance with policy.
Consulted	Who should be consulted in a resource or functional impact scenario?	The CFO or business function controller will be consulted if a backdoor Trojan malware is discovered on a computer used to access financial/ERP applications or data. Specific information about user entitlements and access history will be reviewed to determine associated risk(s).
Informed	Who should be informed of an incident?	The GC will be informed immediately upon discovery of inappropriate access to non-public or privacy information, or systems that contain such information.

Actions

Actions that an organization undertakes to resolve a cybercrime incident or investigation can be as impactful in terms of organizational risk as the cybercrime itself. Legal and regulatory penalties for inappropriate resolutions, which in some cases include very specific disclosures, can financially impact an organization or even result in the prosecution of executives, staff, or related supporting vendors. Similarly, inappropriate or irresponsible disclosure to media or public sources (whether intentional or not) can affect the market performance or perception of an organization and its executive leadership.

It is important to clearly define the role assignments associated with IRP and communication plans, and to include technical remediation actions through testing and scenario planning. Guidance should be documented with recommendations for CIRTs to consider- along with associated RACI- for actions including the following examples:

Table 8-4. Technical Remediation Actions

Action	Example Condition	RACI
Reconfigure	Accounts and related entitlements should be reconfigured for users who have been absent from work for more than two weeks.	MIS (A), IT (A), IS (R), Business Function supervisor (C, I)
Rebuild	A computer that has had malware installed should be rebuilt after release by CIRT.	MIS (A), IT (R), IS (A, I), Business Function supervisor (C, I), CIRT (R, A)
Redesign	If evidence of network architecture or resources mapping is discovered, the affected network segment(s) and supporting ACL' s should be redesigned and implemented as a CIRT escalation.	MIS (C), IT (R), IS (C), Business Function Leader (C, I), Executive Staff (C, I), CIRT (R, A)
Review	IT/OT assets that have configuration anomalies from the organizational baseline should be reviewed for potential evidence of misuse.	MIS (A), IT (R), IS (A, I), Business Function supervisor (C, I), CIRT (R, A)
Retire	IT/OT assets that have had no use, or performed no service, within 90 days of an annual audit should be retired.	MIS (A), IT (A), IS (R), Business Function supervisor (C, I)

●Initial Considerations

How a victim company handles the initial response to a cyber incident is extremely important both to the victim and to law enforcement, for several reasons. It is vital that the company thinks of a cyber incident not only as an IT matter but also as a legal and compliance matter. It is particularly important, for example, that evidence of a suspected breach is preserved so that it may be used to assist with legal determinations regarding breach disclosure obligations under the law, document how an incident was handled for regulators, defend claims by private parties, and - where appropriate- provide law enforcement with valuable clues and investigative leads to identify and stop attackers. As discussed in Chapter 6, methods of evidence collection should involve systemic, automated, and manual capabilities to collect and preserve evidence (including its documentation and handling). Such evidence is often volatile, so it is important to quickly recognize and use tools that support automated or manual acquisitions of related artifacts to associate to evidence. Particularly in large-scale environments, sampling through sweep discovery methods and associated systemic (alerts-based) artifact logging are useful to reduce the vast amounts of technical artifacts that would otherwise be collected with traditional forensic procedures. As mentioned in other chapters of this book, understanding artifacts and sources of evidence and utilizing efficient methods of collection (and analysis) can help organizations resolve cyber incidents.

●Securing the Network While Preserving Evidence

It is important to determine as soon as possible whether an intruder remains in the organization' s network, and therefore whether discussions of the internal investigation or other security measures should continue on the system where an attacker might follow such developments and adapt accordingly. Organizations should consider the use of an approved secure out-of-band communications platform until internal communications are considered "clean". All discussions relating to the incident should be maintained on secure communications platforms and not be made from personal accounts.

Having access to network logs that include access times and locations is essential to identifying which systems have been compromised so that any active breach can be eliminated. Logs are also important in determining which data may have been accessed by an intruder, as well as what may have been removed or "exfiltrated" from the company' s network.

As noted in prior chapters, the points of intrusion and exfiltration may not be the same portions of the network from which data was removed. Attackers commonly seek to move laterally within a victim' s network to identify valuable sources of data and often seek to elevate their stolen user privileges to gain full administrative access to the network. That is why defending a network' s perimeter, although important, is not enough in itself. Instead, firewalls and other perimeter measures must be combined with detection software tools, segmentation of the network, activity logging, and other means of identifying and capturing important data about anomalous lateral movement within the network. These details help to establish the scope and nature of the potential cybercrime.

From law enforcement' s perspective, the preservation of evidence is also an essential issue. Without incident data from the victim' s network, investigators' jobs are made much more difficult. This may also increase the need for law enforcement to request direct access to the victim' s network to attempt to recover forensic artifacts on their own. In the United States, most federal investigators receive special training in obtaining and handling digital evidence. In addition, every major law enforcement organization in the U.S. has invested in computer forensic experts who specialize in conducting very detailed examinations of computer systems whether in a laboratory or on-site, including by mining for data that has been deleted by a user.

Examiners are careful, whenever possible, to work on copies of collected evidence and to not alter it in a way that would render it unusable at trial. When it comes to examining an incident on a victim' s network, even the most highly-trained investigators benefit from the local assistance of the victim organization' s IT personnel who are more familiar with their network. Unlike the examination of a single device, investigating an incident on a large-scale company network usually involves identifying and capturing evidentiary "artifacts" in a network environment that is up and running. It is strongly recommended that computers and related network devices remain in their running state during collection.

Many organizations have in-house investigators who perform a different function than the IT department and are skilled at carefully approaching a crime scene to preserve key evidence, paying attention to evidence handling and chain of custody, and anticipating what law enforcement will request. Additionally, automated software tools are becoming increasingly helpful in capturing relevant incident data and setting it aside for review. Organizations with the resources to deploy these tools on their network as part of an overall incident response plan will benefit from time and resource efficiencies during investigations. These solutions are no longer expensive- free tools serve the same purposes and are as easy to implement and utilize as expensive tools in many cases, as described in Chapter 6). They are practical for every organization today and can provide important time and effort savings for evidence preservation.

As discussed in Chapter 6, It is important to establish and document a chain-of-custody process for evidence collection. The **best evidence rule** is a legal principle which states that the original document is better evidence than a copy of the original, and a copy will not be admissible if the original exists and can be provided. With digital evidence such as massive log files, it is not practical to provide original and all-inclusive logs, files, and hard drives from numerous systems. Further, many large networks use virtual machines, so there is no hard drive per se to remove, copy, and provide to law enforcement. Therefore, a process to ensure that collected evidence is not modified or changed in any manner is critical. Forensic software can automate the collection process. Specific transactions in log files may be extracted from larger data sets after filtering out irrelevant data from collected evidence, so long as investigators document (and are willing and able to testify, if the case requires it) their evidence collection and analysis procedures. Accordingly, investigators should review collection and chain-of-custody processes with legal counsel(s) to ensure they will be able to withstand scrutiny during a court proceeding.

●Documenting Response and Remediation

How a company documents its response to a cyber incident is extremely important from a legal perspective. The process of identifying indications of cybercrimes should be systemic, with alert-based logging and associated tools and procedures to collect evidence. Those procedures must include evidence handling and should specifically include "case management" documentation. It is strongly advised that CIRTs contain a formal scribe to ensure that decisions and actions are formally recorded for later review. Whether an investigation is initiated by an alert from a logging system or on advice by counsel, the documentation should essentially be the same as a standard organizational procedure.

Whenever possible, the company' s in-house or outside counsel should direct the investigation so that attorney-client privilege and (in the United States) attorney work product protections cover the investigative summaries and conclusions. This approach should apply to all significant steps in the investigation, including interviews with company personnel regarding the incident. Although privilege and work product protections are likely to face challenges in litigation and are far from infallible, they give the company a strong chance of protecting its sensitive analytical work. Although the underlying facts cannot themselves be privileged and witnesses may be directly called to testify in court proceedings, the company' s own efforts to understand what happened and how they may be protected from disclosure can, in many circumstances. Outside counsel generally has (much) stronger protection of privilege than in-house counsel, for the simple reason that in-house counsel represents executive management functions of the organization that necessarily factor into investigations.

It is also important to attend to the manner in which the results of an investigation are written. The company' s investigators or outside forensic vendors sometimes fail to consider the effect of what they write on civil litigation and regulatory proceedings which may occur long after their work is done. For that reason, the language of the report is something that counsel should evaluate before the report becomes final. Ensuring that the results are written carefully and avoid exaggerated language, an unnecessarily expansive scope, and unduly dogmatic conclusions is yet another layer of protection when the company' s actions are tested by civil litigators, regulators, the media, and others.

These legal considerations have important implications for law enforcement because they affect when a victim will report a cybercrime and what evidence they will agree to turn over to investigators. The best practices in documenting evidence are to be factual and brief, to use terms such as "based on current understanding" (interpretation should not be included in documentation-that is the domain of expert witnesses and the courts), and to never speak in absolute terms. Investigators can never know everything about anything, so recognize that <u>what is being documented</u> is only <u>what the investigator is observing and doing</u> at that time. There will always be others doing the same.

●Providing Evidence to Law Enforcement

Because of the liability concerns discussed above, a corporate victim of cybercrime must be careful about the information it provides to law enforcement. Every effort should be made to give law enforcement the information necessary for them to do their job without compromising privilege and work product protections or otherwise unnecessarily exposing the company to liability down the road. Information does not necessarily mean data, however.

Information and data are different. Sometimes due to scale or sensitivity/liability issues, data will only be summarized by approved experts such that the legal responsibilities of the investigators and the organization are not violated. For example, in the vast majority of cases law enforcement does not need—and therefore should not be requesting—the content of communications occurring on the company' s network. Instead, law enforcement most often needs only log data and other non-content information necessary to determine how, when, and where the intrusion occurred. Some exceptions exist, such as the content of a phishing email which may provide clues to the identity and modus operandi of the attacker. Under U.S. and many international laws, communications that are part of the crime itself rarely present a legal barrier to the victim in providing these items to law enforcement, but legal guidance should be sought and the basis for providing network data and communications to law enforcement should be documented.

●Cyber Investigations are Not IT or IS

A crucial distinction in cybercrime investigations is the recognition by the organization that cyber investigations are about investigating crimes – not simply information security or technology lapses. Cybercrimes can result from misconfigurations of systems and applications, but they are intentional violations of laws with objective outcomes. Considering a "Banker Trojan" infection of a controller' s computer an IT/IS issue is not correct, and rebuilding that single system may not resolve the more important issue – that an intruder first somehow made their way into the network to selectively install the Trojan to commit financial theft or fraud. Investigations require different actions.

Procedural Remediation

Procedural remediation is as important as technical remediation. How an organization is to resolve a cybercrime incident is fundamentally dependent upon the nature and scope of the crime. The process of procedural remediation is visualized in Figure 8-6 below and described in this section.

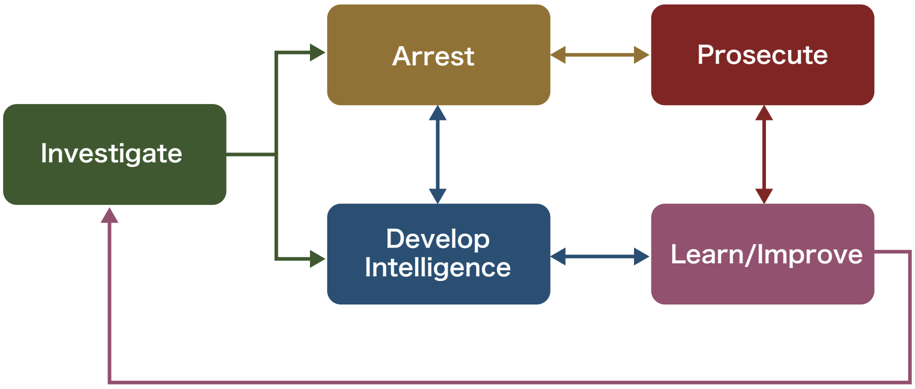


Figure 8-6. Procedural Remediation

Investigate

Investigating cybercrimes is more than just reviewing alerts in a SIEM and removing malware from infected computers. Investigations involve determining the scope and objectives of a cybercrime such that effective resolution can be achieved. In some cases simple remediation will be achievable, and organizational policies should define what conditions those cases can invoke. In other cases, particularly where non-public, private, or protected information is accessed without authorization (or shared/stolen), specific investigative procedures must be performed. Those procedures should adhere to evidence collection and handling processes under privilege and with appropriate chain of custody documentation.

●Review of Sources of Evidence

After the initial response to secure the victim' s network- ensuring there is no remaining active breach or backdoor access by cybercriminals, documenting technical remediation steps, and collecting key evidence- the investigation must review sources of evidence to try to determine criminal intents or interests. Clues gathered from the victim' s network can often be combined with information from other sources that were described in Chapter 5, such as:

- **Known malware** samples, attack indicators, and other **"signature" data** gathered by investigators in other cases. Because cybercriminals typically use the same tools, infrastructure, and methodologies in a series of attacks against multiple victims, investigators will often already have valuable information that can be compared with evidence collected from the victim' s network.
- Analyses published by the **cybersecurity research** community, including by firms offering forensic services. For example, security researchers have published detailed analyses of various malware campaigns and of cybercriminal infrastructure including botnets: networks of compromised computers under the control of botmasters, which are used to carry out everything from denial of service attacks to the exfiltration of stolen data. This type of information can also include community information sources such as Virustotal[266] or similar services.
- Evidence obtained from **third parties**, such as communications service providers who are sometimes innocent owners of intermediate "hop points" used by cybercriminals, financial institutions who are used to launder stolen funds, and others. While some third-party data may be obtained by consent under local law, in most jurisdictions law enforcement must obtain and serve subpoenas, court orders, search warrants, and other compulsory legal processes to the third party. These services are designed not only to compel production of relevant information, but also to protect the third party from claims of privacy violations for disclosing customer data without lawful authority.
- Evidence obtained through new and existing **undercover operations** and through cooperation by participants in those activities, such as confidential informants. This is a growing area of importance but also carries significant legal concerns that depend on related jurisdiction(s).
- Evidence obtained from **investigators in other countries**. Because the evidence of cybercrimes is rarely confined to one country, cooperation with foreign law enforcement is extremely important.

[266] https://www.virustotal.com

The last three categories are discussed in greater detail below.

●Evidence Held by Third Parties

Using clues from the victim' s network, investigators may identify leads for other potential sources of evidence. In the early days of cybercrime, obtaining and following an Internet protocol (IP) address (or series of addresses) often led directly to the computer used in the crime. Today, attackers typically use a series of third-party "hops" that cross international/jurisdictional lines and leverage encrypted channels of communication such as virtual private network (VPN) services. This complicates an investigation, requiring consideration not only of the "digital trail" but also the financial trail, similarities to other incidents, existing knowledge of the infrastructure and actors, and creative undercover operations. Investigators should therefore create an initial list of the third-party sources for which they have leads (derived from the crime) and determine which legal tools are available to gather evidence from those sources.

In the United States, the legal tools available to cybercrime investigators are largely the same as those available in other non-cyber cases. Although an entire book or course could be devoted to the available legal authorities in any one jurisdiction, by way of general overview the key evidence gathering tools in the U.S. include the following:

- **Grand Jury Subpoenas.** A subpoena is not the same thing as a **court order**. It is a legally binding demand for evidence issued by a prosecutor under the authority of a grand jury and enforced by a court. If the party receiving a subpoena fails to comply or seeks to challenge the legality of the subpoena, a court decides those issues. In the U.S. a subpoena is used in a cybercrime case to request basic non-content information such as the name, address, and billing information of a subscriber for a particular account. More expansive non-content data such as web log data usually cannot be obtained by subpoena and requires a court order.
- **Search Warrants.** A search warrant, issued by a court based upon shown "probable cause" (that is, a reasonable belief that evidence of a crime exists at a particular location), allows the authorized law enforcement officer to enter a physical location or to search a physical computer or device/equipment for specific categories of evidence set forth in the warrant. In the context of computer evidence, search warrants are used to obtain stored data including content but do not allow the interception of content in live communications.
- **Wiretap Orders.** Wiretaps have long been used in many jurisdictions to intercept live communications. In the U.S., they were initially used decades ago in organized crime cases but are now commonly used in narcotics cases and increasingly in cybercrime cases. Because of the significant intrusion into the privacy of the communicants, U.S. law allows wiretaps only upon shown necessity, with a plan to minimize the risk of intercepting irrelevant communications and with frequent update reports to the court.

The legal requirements for evidence collection and production are sometimes confusing and should always be clarified based upon advice of counsel. That advice, though, should form operations policies that define CIRT staff job functions and performance. For example, the following ECPA service guidance (shown in Figure 8-7) refers to email[267], which is only one source of evidence that may be required in a cybercrime investigation.

Figure 8-7. U.S. Service Requirements on Email Collection

Type of Communication	Required for Law Enforcement Access	Statute
Email in Transit	Warrant	18 U.S.C. § 2516
Email in Storage on Home Computer	Warrant	4th Amendment, US Constitution
Email in Remote Storage, Opened	Subpoena	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for 180 days or less	Warrant	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for more than 180 days	Subpoena	18 U.S.C. § 2703

●Undercover Operations

Beginning in the early 2000s, cybercriminal groups began to take shape, building on the early black market "carding forums" of the 1990s in which stolen credit card information and other data was traded. Over time, these groups have reached an impressive level of sophistication, pulling together individuals with a range of specialized skills necessary to take on high value hacking targets. More recently, some groups have added subject matter expertise to their schemes to maximize the access they have gained for specialized tasks such as trading on stolen inside information, navigating industrial control systems, or executing an electronic payment/wire transfer on bank payment networks such as SWIFT[268]. In fact, the top cybercrime groups in the world are organized crime groups that rival the capabilities of the vast majority of nations. This is largely driven by the interests that subscribers to those cybercrime proceeds have demonstrated. Cybercrime as a service (CaaS) (as previously discussed) represents the growth of a market response to a request. By utilizing CaaS, subscribers can gain access or advantage with some measure of anonymity.

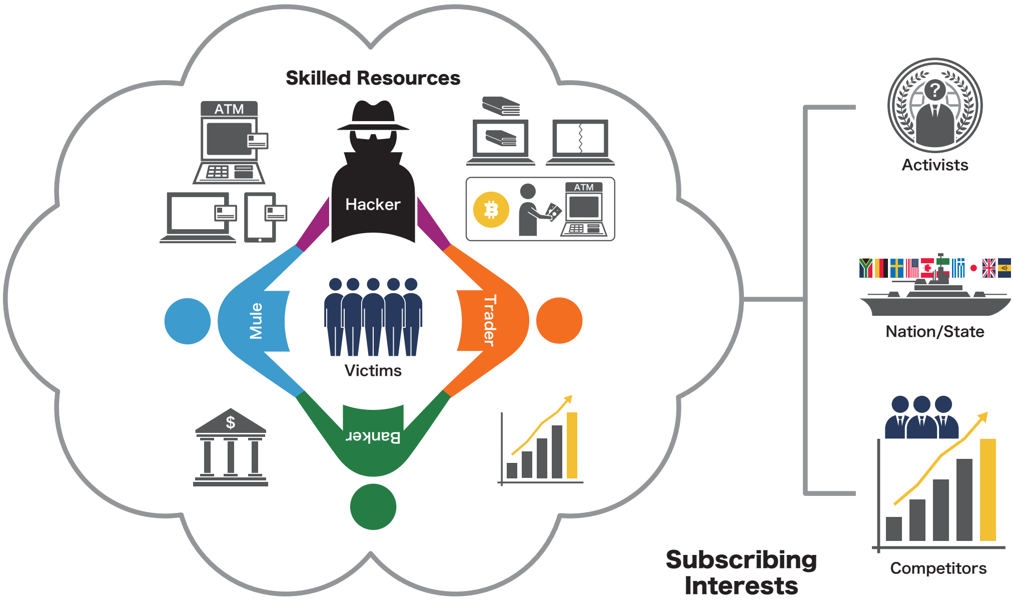


Figure 8-8. Cybercrime Environment

[267] https://epic.org/privacy/ecpa/

[268] https://www.swift.com/

In light of the progression of cybercrime into organized crime, many years ago U.S. law enforcement began to use the same types of undercover operations it has utilized against traditional organized crime groups. This includes a long-term strategy to identify and follow the activities of group members, including through the use of wiretaps and other invasive investigative techniques commonly used against mafia groups and drug gangs. Just as police have done for years in mob and drug cases, this also may involve infiltrating the group itself or otherwise interacting with its members in an "undercover" capacity.

As with those traditional cases, it is also typically the case in cybercrime that those most likely to be identified and arrested are lower ranking members of the group: often, those involved in the more exposed "cash out" portion of the scheme. So-called "money mules" and other low-level members, once arrested, can choose to cooperate and continue in the scheme under law enforcement monitoring and supervision in order to assist in identifying other members of the group. A crucial legal tool in this effort is plea bargaining: providing credit for cooperation against a defendant' s sentence (or noting cooperation to the court, including in closed proceedings) in exchange for the cooperation itself. Through the use of these techniques, U.S. law enforcement has succeeded in gaining consensual access to cybercrime group communications and valuable insights into its future operations.

One reason that undercover operations can be important is that cyber is sometimes only a means of achieving an objective. In organized cybercrime, the perpetrator may not be the hacker; they could be any party associated with the organized activities. For example, some CaaS cyber partnerships involve initial access brokers selling credentials to extortion gangs; in these cases, the extortion gangs are the perpetrators and are enabled by access brokers. Once a significant percentage of the group' s members have been identified the prosecution usually becomes public, resulting in the disbanding of the crime group. Some members may escape prosecution and go on to other schemes, but their activities will have been disrupted significantly and they will likely experience a real fear of getting caught.

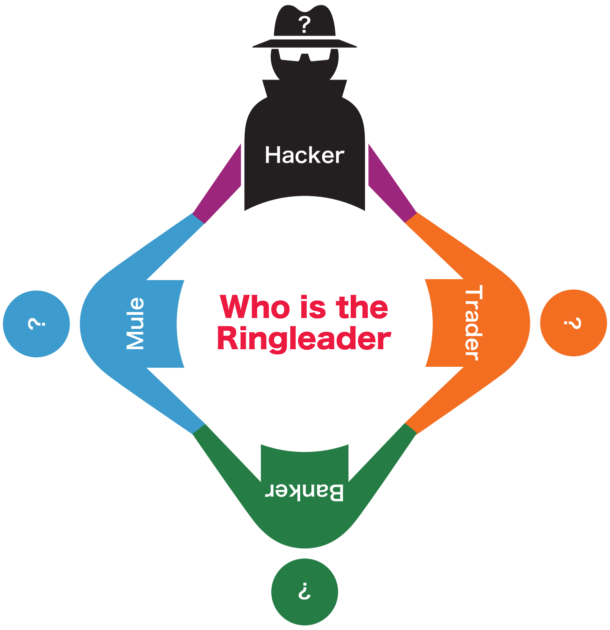


Figure 8-9. Organized Cybercrime

There are several important legal considerations in undercover operations. For example, in cybercrime cases, a significant consideration is the fact that servers and defendants may be located in other countries. Another consideration is the type of criminal activity law enforcement will be participating in: allowing a fraud scheme to continue for a brief period in order to identify the criminals behind it may be worth the costs and risks; allowing an online child pornography ring to continue while observed by undercover operators may be another matter. It is also important to consider the risks undercover personnel will be taking and how they will be managed. These and many other important legal and practical issues must be considered carefully in accordance with local law.

Eventually, however, a pattern of acceptable practices begins to emerge which provides investigators with a basic roadmap to design and carry out legally-defensible and effective undercover operations. Organizations should set up clear rules and guidelines and a rigorous and consistent system of review, to ensure that any such proposed operation is evaluated and, if authorized, monitored and documented with great scrutiny in accordance with safety, legal and policy considerations.. It is wise to involve supervisors with specialized knowledge of cybersecurity and privacy issues in such review and monitoring; this should certainly include legal counsel and law enforcement in the design (and, critically, the approval) of any such activities.

●Obtaining Evidence from Other Countries

Very few cybercrimes occur entirely in one jurisdiction. In addition to the legal authorities for evidence gathering discussed above, investigators will often need to request assistance and formal evidence from other countries. As discussed in Chapter 1, formal evidence requests are typically made pursuant to terms of the Budapest Cybercrime Convention[269] or Mutual Legal Assistance Treaties (MLATs) between countries. These treaties tend to have common provisions such as: a formal list of the types of crimes to which the treaty will apply; “dual criminality”, the requirement that the receiving country have a similar criminal provision to the one that forms the basis for the request; and a national security exception where the receiving country may decide not to provide requested evidence for national security reasons.

“Treaty 185” of the Budapest Cybercrime Convention provides a mutual agreement of signatories concerning definitions of certain cybercrimes and coordination among related law enforcement agencies. It is by no means a “global” treaty, as only 49 countries are signatories and 49 countries (not all the same ones) have ratified and entered into the agreements– though 27 indicated their reservations and 25 made declarations.[270]

[269] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[270] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

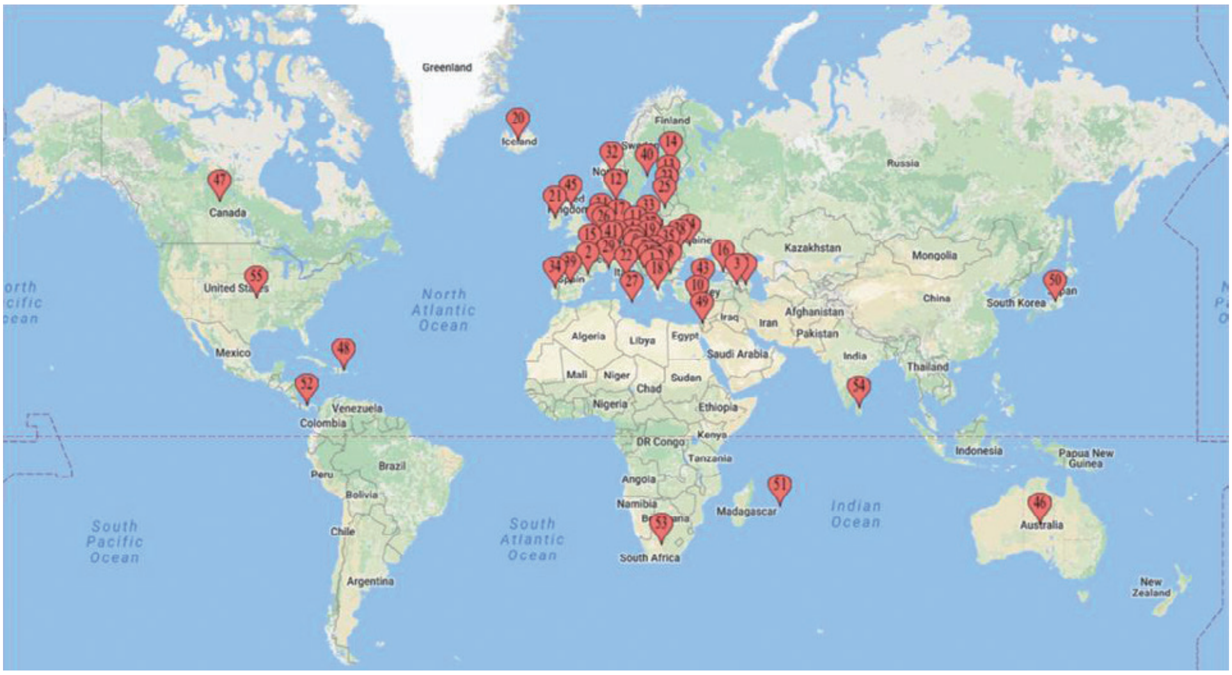


Figure 8-10. Signatories of Treaty 185

The MLAT process of sending and responding to requests is notoriously slow and highly bureaucratic. A typical time frame for receiving requested evidence is many months, although some countries with trusted relationships and similar legal frameworks are able to honor requests more quickly. Despite their flaws, MLATs are frequently a necessary step as they are often the only means of obtaining formal, authenticated evidence from another country that can be used in a trial. They are not particularly effective, however, for obtaining evidence quickly enough to identify and stop cybercriminals who operate at light speed and who tend to constantly change communications channels. To achieve these goals, where permissible investigators work through "police channels," in which they ask their law enforcement counterparts to provide police intelligence about the ongoing crime (this is not the same as national security intelligence, which is another matter altogether) or to take proactive investigative steps under local law.

Sometimes, local law enforcement is able to identify a jurisdictional basis to open its own investigation domestically and take such steps, and to share the results with the requesting foreign investigators. This same approach is taken in many other types of serious cross-border cases, most notably counter-terrorism cases in which waiting many months to take action to stop the crime is not an option. In such cases, formal evidence exchange for trial can occur later and the immediate priority is stopping serious harm. Only by proceeding on these dual tracks—a police channel for rapid intel exchange and action on the ground, and a formal MLAT process for the eventual day in court—can law enforcement maximize its ability to disrupt cybercriminals.

Arrest

Arrest and charging a suspect with a crime are related but different concepts. The process of arrest involves locating and physically restraining an individual suspected of a crime. Charging may or may not coincide with an arrest. Either may come before the other, but an arrest also might never result in a charge.

Given that cybercrimes tend to cross jurisdictional lines with perpetrators, victims, and computer infrastructure located in varied countries, there is often more than one jurisdiction in which charges can be brought. Such decisions are highly specific to the facts of a situation. For example, when the defendant is a citizen of the jurisdiction in which he conducted hacking activity that affected victims in another jurisdiction, his home jurisdictional authorities will often prefer to prosecute the case rather than extradite one of their nationals. Indeed, several jurisdictions have constitutional or policy prohibitions on the extradition of their nationals (the United States has no such general prohibition).

On the other hand, authorities in the jurisdiction in which the victim(s) are located have a strong argument that justice is most appropriately served by the prosecution proceeding in its courts, particularly where victim testimony and other domestic evidence are central to the case. It is also possible for prosecutions of different but related crimes to proceed in both jurisdictions, although as a practical matter the delay associated with waiting for one proceeding to conclude (including appeals processes, which can take a long time) can make that approach challenging.

●Charging Considerations

Many jurisdictions now have a criminal statute specific to computer hacking. In the United States, the relevant federal statute is known as the Computer Fraud and Abuse Act (CFAA).[271] At the center of the CFAA are the concepts of "access[ing] a computer without authorization or exceeding authorized access." The CFAA is now quite dated (as it was enacted in 1986) and is showing its age in the modern era of digital crimes, though the concepts it includes have thus far survived. That said, many prosecutors have successfully convicted a computer hacker for violations of other criminal laws not specific to hacking, such as laws involving fraud, money laundering, identity theft, theft of intellectual property, criminal conspiracy, and so forth.

Rather than focusing on unauthorized access, most other cybercrime laws focus on the objective or intent of the cybercrime activity (currently still loosely defined as "hacking"). In some cases, those crimes are easier to prove than a computer hacking charge under the CFAA, or they may allow for greater penalties and may be added to- or charged in lieu of- a CFAA charge depending on the facts and circumstances of the case.

Besides identifying criminal laws with the most readily provable elements to address the defendant's activities, there are also considerations regarding: the possible sentence; the nature and scope of evidence that will be necessary to present at trial if a particular charge is included; whether and how damages must be proven; and the ability to defend searches, seizures, and other evidence gathering techniques underlying the evidence. It is also usually a wise practice to understand what sensitivities, from the victim's perspective, may come into play if certain evidence were presented in a public forum. While prosecutors cannot give a victim the right to draft or edit an indictment, they certainly can and should take into account the victim's interests so as not to victimize them twice. In effect, they can be re-victimized by an ill-considered charge that requires unnecessarily sensitive testimony, or via other evidence from the victim concerning its network systems or otherwise. Careful consideration of these issues maximizes the chances that the victim and others who learn about their positive experience with law enforcement will be more likely to cooperate in future cases.

[271] https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf

●Issues Specific to Cybercrime Arrests

When carrying out the arrest of a cybercrime suspect, investigators should take great care to preserve the digital evidence both in the defendant' s physical possession at the time of arrest as well as evidence the defendant could alter remotely (or instruct someone else to alter) once he or she realizes what is happening. Another important consideration is the fact that the perpetrator may act to encrypt the devices in their possession. Devices may also simply time out on their own, costing investigators the chance to secure valuable evidence. This may be caused by intentional acts such as those performed by ransomware actors, or unintentional configuration issues such as computer "shutdown" settings. For these reasons, in addition to the usual safety concerns involved in any arrest, investigators must carefully plan their strategy for preserving digital evidence at the time of arrest. This new reality means that all investigators should receive basic training in the handling of digital evidence. Typically, as is the case when approaching a cyber incident on a victim' s computer network, investigators will also want to have at least one member of the arrest team who is specially trained in computer forensics tools, methods, and rules.

Because there are a number of legal issues associated with law enforcement' s seizure of and access to the devices found in a suspect' s possession, law enforcement should involve a prosecutor early in the arrest planning process so that these issues can be thought through ahead of time whenever possible.

Develop Intelligence

It is important to recognize that the most adept cybercriminals tend to make a career of cybercrime, moving from one scheme to another over time. Cybercrimes involve learning new technologies and methods through a considerable amount of research and testing, and cybercriminals will suffer unsuccessful attempts to perform cybercrimes. Technologies will change along with attack methodologies, but the people behind the most serious cybercrimes tend to continue their "business" with others they have developed relationships with. This is why law enforcement must not simply follow digital trails left from every cyber incident, but must also take a long-term view that pays attention to the individuals involved in a series of cybercrimes. Identifying these individuals (that is, making "attribution") is usually not a short-term proposition but instead involves mapping relationships among cybercriminals and the infrastructure they use, looking for patterns of activity, and developing sources and undercover operations to provide insights from inside cybercrime groups. By developing their knowledge of these individuals and groups, investigators can have a head start in identifying cybercriminals and apprehending them.

The best cybercrime investigators and prosecutors also tend to make a career of it, amassing specialized training and building key relationships worldwide with other investigators and with potential victims in their respective jurisdictions. These relationships of trust are the foundation of successful cybercrime investigations and law enforcement operations. Investigators who are serious about building expertise and capacity to address cybercrimes should take advantage of opportunities to train with law enforcement from other jurisdictions, including by attending leading conferences where everything from fundamentals to cutting-edge issues are discussed. Perhaps even more valuable than building knowledge, however, is the working relationships that are forged through these exchanges of expertise.

Investigators must also realize the limits of their knowledge. This is particularly important in regards to attribution. Attribution based upon post-incident investigation is less likely to return accurate identifiers of individuals than attribution based upon intelligence which identifies (through monitoring) the initiation or activities of an ongoing cybercrime. Relevant privacy issues in investigations include false charges or even mis-attribution (if published) that can lead to civil or tort claims of libel, defamation, or "false light" etc.

Of course, the disruption of cybercrimes resides not only in governments but, perhaps even more so, within the private sector which controls the vast majority of Internet infrastructure. In the United States, the push for companies to share cyber threat data among themselves and with the government is designed to enable better defenses, which ideally can adjust in real time through machine-to-machine sharing of threat indicators. Although the human element of fighting cybercrime is not going away, the more tools that are brought to bear in the fight the less surface area and less damage that can be caused. As companies and governments become better at designing and protecting systems and defenses, cybercriminals will be forced to expend far more effort and resources. Their activities will leave more artifacts and evidence to identify perpetrator(s) and lead to arrest and charges.

Prosecute

Judges and juries in the United States are now used to seeing computer evidence presented in court by both the prosecution and defense in criminal trials, as well as in civil trials. In many other jurisdictions, however, this type of evidence may be new and the lawyers involved may need to plan for additional time to explain how the evidence was acquired, how it can be trusted as authentic, and exactly what it means.

Even in the U.S., this is still a practical approach. The good news is that the social media and smartphone age has led to computer technology becoming a daily part of the lives of many citizens, so they are usually not intimidated by the prospect of working with such evidence in a trial. The challenge, though, is that technology has made user interfaces so convenient and mindless that many still do not comprehend what is happening behind the scenes when they visit a website, send an email, or post something to their social media account.

Prosecutors and investigators should use these opportunities to teach judges and jurors about the workings behind the scenes and the residual artifacts (clues) left as a result. They will typically find an audience that is very eager to learn about the technology which is such a big feature in their daily lives.

A larger challenge arises in presenting more complicated computer forensic testimony at trial, which is usually delivered by someone qualified as an expert under the law of the jurisdiction. Some of this challenge is due to confusion around the varied types of witnesses that might be called in a trial. The following table provides some clarifying details:

Table 8-5. Types of Witnesses

Type	Description
Investigator	A law enforcement officer who provides fact-based testimony limited to their observations and actions, supported by documentation they created or reviewed.
Fact Witness	A substantive testifying expert who has personal factual experience with a subject system, process, or document produced as an exhibit. Law enforcement officers often serve as fact witnesses (only the facts). Supervisors or programmers of processes, functions, or systems that support the same for organizations may serve as fact witnesses on specific issues subject to their personal knowledge.
Expert Witness	A "qualified" expert in a field of knowledge designated by the court in each case specific to the case issue(s). This expert will be examined by both parties' counsel as well as the court, and sometimes by the jury via the court. The judge will ultimately decide the acceptance or rejection of an expert witness. The court relies upon expert witnesses to describe technical concepts or valuation of damages. The expert witness provides an opinion based on knowledge, experience, and education.
Lay Witness	Lay witnesses are witnesses who provide answers to questions posed by counsel or the court. Their answers are based on observations; law enforcement officers may serve as lay witnesses.
Consulting Expert	Consultants to assist counsel with trial preparation, evidence collection and analysis, and review are considered consulting experts. Consultants who work for a company rather than under direction of counsel are not designated experts. Consulting experts may serve as fact witnesses.
Deponent	A deponent provides deposition testimony as a sworn witness – either lay, expert or fact as the situation (and qualifications as presented but not yet accepted) requires.
Plaintiff/Defendant	The parties to a case, represented by counsel.
Victim	A victim of a crime may be a deponent or a lay witness.

It is a tactical decision at the outset whether or not to qualify a witness (fact or expert) to present the testimony at hand. In the U.S., investigators are usually capable of presenting fact-based testimony except where the forensic evidence is particularly complex (or very complex methods were used to obtain it). In those situations, the defense will typically stipulate the authenticity of the forensic copy ("image"), which is easily proven through a cryptographic hash value comparison showing that the copy examined is identical to the content of the device at the time it was seized.

The more technical the digital examination process of the evidence at issue in a case, the more likely that testimony from a qualified expert witness will be required. When this occurs, prosecutors should be sensitive to the fact that computer examiners tend to speak in technical terms, although those with significant experience on the witness stand will have learned how to make technical concepts accessible to laypeople. It is important for prosecutors to demonstrate to the jury a rigorous and trustworthy process that generates certain digital artifacts. This is usually done through testimony of fact and expert witness testimony. The best expert testimony comes across as truly agnostic to the results, so that the witness does not appear to be arguing for a particular outcome.

Prosecution of cybercrimes depends upon the following to educate the court and jury:

- Legal evidence collection and reliable analysis techniques
- Analytical results that provide proof of violation of specific laws
- Presentation of the facts and opinions of witnesses
- Associated (potential or real) harm to a victim

Learn and Improve Detection/Prevention of Cybercrimes

Any process can be improved with practice. This includes the process of resolving cybercrimes.

Organizations should document successes as well as problems they face in the process of remediating associated issues. They should also seek to constantly improve communications to ensure stakeholders (RACI) have actionable information that provides value to their support or decisions as required. Improvement means creating efficiencies of scale and economies of related resources.

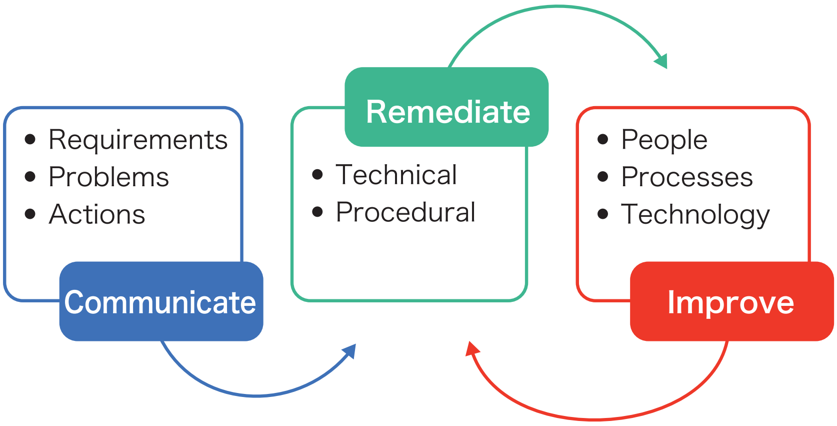


Figure 8-11. Improving Resolution

As a CIRT proceeds through an incident, it may become necessary to manage barriers to communications or faults in procedures. These tactical improvements should be documented for after-action review and program improvement. The organization' s strategic capabilities to detect, prevent, or respond to cybercrime incidents will thereby improve with practice and experience.

Chapter 8: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

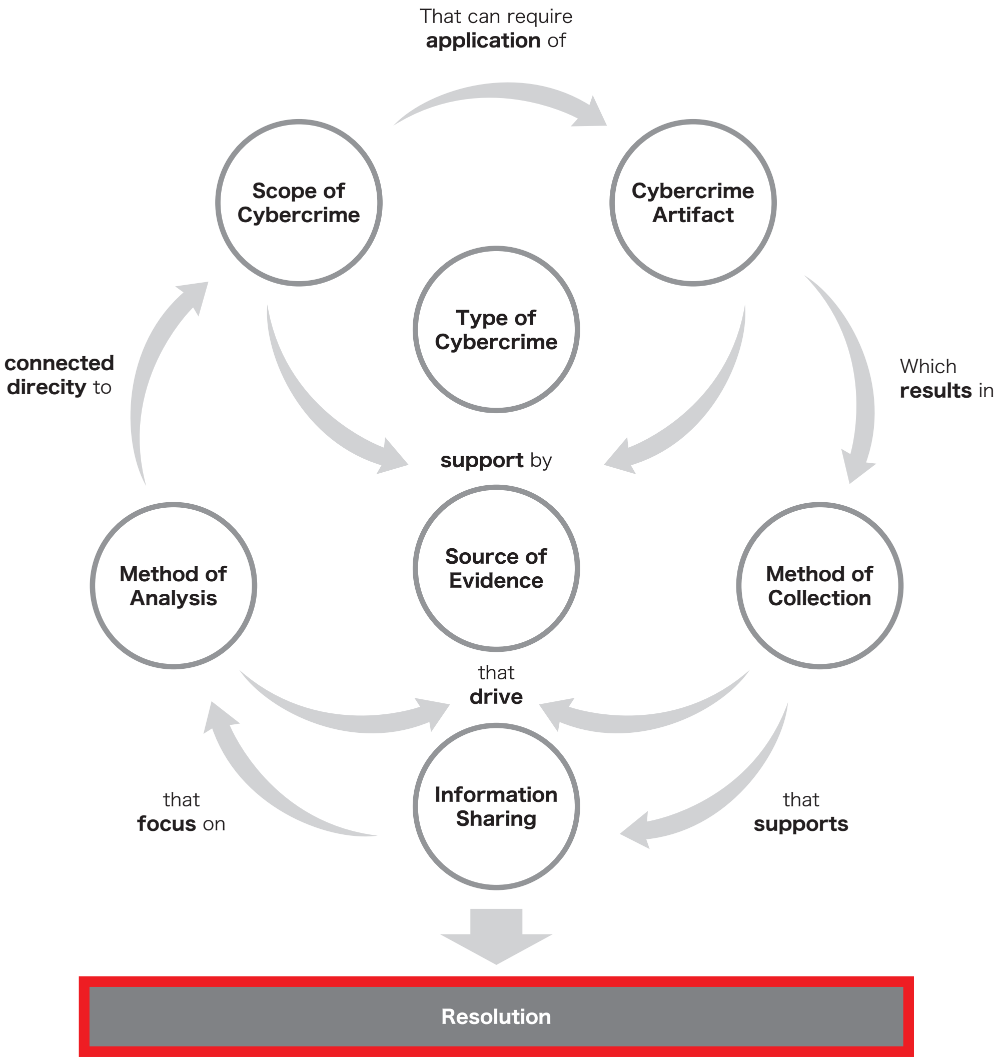


Figure 8-12. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 8-13. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 8-14. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should plan, document, and direct resolution activities.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. To achieve effective resolution of cybercrime incidents, intelligence should monitor sources and assist investigators by supply or discovering applicable IOCs.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigators must demonstrate tactical knowledge of requisite evidence collection and handling, and analysis to assist judiciary with prosecution; and to support the organization in necessary technical and procedural remediations.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will dictate the approach to an investigation as well effective prosecution and/or remedial activities to resolve cybercrime incident.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The scope of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when, according to which organization/functions/personnel are affected. Public relations must coordinate with the judiciary to ensure effective communication with appropriate external agencies, according to legal limitations.

Support – require procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 8: Review

1. How should a cybercrime investigation and resolution function be organized?

   Answer: By a CIRT, including executive and business functional sponsorship

   Examples: CIRT leader, Inside/Outside Counsel

2. What are the components of a business impact assessment?

   Answer: Assets Inventory, Risk Register, Contingency Plans, Resource Interdependencies Map

   Examples: CMDB, Risk Register, BCP/DRP, etc.

3. What are the ABC' s of cyber security?

   Answer: Attacks on Resources and Assets, Breaches of Controls, and Compromises of Functions and Data

   Examples: Phishing, Penetration Attacks, Social Engineering, Backdoor Trojans, InfoStealers, Fraud, etc.

4. What methods of communication, and with what authority, should be established for phases of cyber investigations and resolution?

   Answer: Systemic and incidental communications (including IRP and Red Book)

   Examples: RACI to reconfigure, rebuild, redesign, review, and retire

5. Who should be involved in cybercrime investigation and resolution program functions, and when?

   Answer: Determine roles using RACI: Investigators, CIRTs, experts, Counsel, etc; should entail Communicate, Remediate, and Improve

   Examples: Communicate throughout the process, remediate according to guidance and sensitivity/risk, improve with lessons learned

6. What tools, personnel, and procedures should be aligned for resolution?

   Answer: Alerting, digital evidence collection, and CIRT (plus investigators and experts)

   Examples: Secure the network, collect evidence, investigate and prosecute the crime to detect and respond or to prevent future incidents

Case Study 8: Resolving an Incident

- **Crime**: Business Interruption
- **Suspect(s):** Employee
- **Means:** Ransomware
- **Motive**: Sabotage
- **Opportunity**: Access to sensitive operations

An automotive assembly line worker named John Smith was accused of attempting to deploy ransomware on the company's manufacturing and assembly network. The initial accusation stemmed from suspicious activity detected on the network and the employee's computer being flagged by the company's cybersecurity systems that were monitored by a third party services provider. However, as the investigation progressed, it became increasingly apparent that the evidence supporting the accusation was incomplete and inaccurate, creating a complicated and controversial scenario.

The cybersecurity team's initial analysis suggested that ransomware had been deployed based upon indicators of compromise associated with Smith's workstation by the third party cybersecurity services provider. The incident logs from their SIEM indicated that the employee had inserted a USB drive into his computer and caused ransomware to be installed, which raised immediate red flags and called for swift action due to the potential of infecting other computers in the assembly network. In response, the company's IT department isolated Smith's workstation and suspended him pending further investigation. This swift decision was driven by the gravity of the potential threat posed by ransomware, which can encrypt data and halt production lines, causing significant financial and operational damage.

Following the suspension, a comprehensive forensic analysis of Smith's workstation was conducted. The forensic team made use of advanced tools and methodologies to extract and analyze data from the employee's computer. During this process, every aspect of the workstation's activity logs, file history, and network connections was scrutinized and compared against the third party's SIEM data.

Initial findings from the forensic analysis contradicted the earlier conclusions drawn by the third party cybersecurity services provider. The evidence collected from Smith's workstation showed discrepancies in several key areas. First and foremost, while ransomware was discovered on the computer, it had been caught and neutralized by EDR software. Additionally, the forensic evidence contradicted the SIEM logs from the third party. The forensic evidence from the workstation clearly detailed that Smith had merely opened a Chrome browser and performed a Google search for a nearby deli. A malicious advertisement was returned by the browser when he selected a Google search link, that exploited a vulnerability in the (unpatched) version of the Chrome browser that he was using. That caused the automated download and attempted installation of the ransomware. In fact, no USB had been used by Smith or anyone else with that workstation.

Examination of the third party SIEM logs detailed certain anomalies related to redundant proceses and times. The analysis revealed that in fact the logs were a combination of two different computers, each performing different processes that were being monitored at different times, but having the same IP address assignment. The SIEM log was configured to identify hosts by IP address and time correlations, but the two separate computers' information that were contained in the merged log had been assigned the same IP - from independent organizational network segments. The use of a USB device was coincidental in time, but by a user of another workstation in a clerical function, and was not suspicious. These revelations cleared Smith.

Another significant finding stemmed from the malware analysis conducted by the forensics team. The ransomware sample matched several signatures of known variants, but a deeper dive revealed that this particular strain had been properly detected by the organization's EDR.

The outcome of this thorough investigation highlighted several important lessons for the company and wider industry. First, it underscored the necessity of comprehensive forensic methods in cybersecurity investigations, ensuring that initial findings are meticulously verified before any punitive actions are taken against individuals. Second, it demonstrated the importance of understanding the data that third party cybersecurity services providers rely upon.

In light of the investigation's results, the company took several corrective actions. John Smith was reinstated with a formal apology, and the incident prompted a reassessment of the company's cybersecurity strategies and incident response protocols. The IT department implemented advanced monitoring tools, isolated the assembly network from the internet and other functional areas of the organization, and conducted scheduled and regular training sessions to detect and respond to sophisticated cyber threats more effectively. Additionally, the company initiated a collaborative effort with external cybersecurity experts to enhance their defenses and ensure such misconceptions do not occur in the future.

Ultimately, the case of John Smith illustrates the complexities and challenges inherent in cyber-related investigations within industrial settings. It reinforces the critical nature of taking a methodical and evidence-based approach to cybersecurity incidents, ensuring that justice is served accurately, and valuable employees are not wrongfully implicated.

Chapter 9

Cybercrime Information Sharing

Introduction

When a cybercrime is committed, evidence of the activity is typically left either intentionally (defacing a web page, publishing confidential information, etc.) or inadvertently (an IP address logged by a sensor, a malware binary, etc.). When law enforcement or other investigators initially respond to the crime, the initial available information may be sparse, particularly if the attackers have used sophisticated techniques in an attempt to cover their tracks or if the original activity began some time ago. By following an orderly incident response (IR) process, ensuring proper chain of custody, and using the forensic and IR techniques discussed in the preceding chapters, additional information and evidence will be generated. Such data may include details of the tactics, techniques, and procedures (TTPs) used by the attackers as well as information useful for attribution (identification of the individual or group behind the crime) or for understanding or ascribing motive(s).

This evidence can be helpful to investigators as they build experience for future cases and efficiencies for analysis and prosecution. However, the evidence only represents artifacts for the specific victim. Because of today' s "sharing" economy of knowledge, skills, and resources (even infrastructure), and the organization(s) of cybercrime, it is unlikely that the artifacts discovered at a single victim location will reveal enough about a cybercriminal to enable identification or effective prosecution. It is primarily for this reason that information sharing is so important in cybercrime investigations. If shared, such evidence can help organizations identify artifacts or indicators of early activities that, if responded to, can ward off subsequent crimes. Certain types of crime necessarily limit the types of information that can be shared, due to sensitivities of privacy or investigatory details crucial to the discovery of additional evidence for prosecution. In other words, not all information that may be helpful can be shared when it might actually be useful for interrupting cybercrimes.

Since 2013, cybercrime information sharing has expanded through varied methods and venues. New models have been defined to describe cyber risks and threats, and impact information sharing has become a helpful tool to comprehend the immediacy of cybercrime risk indicators for organizations. The quick dissemination of information is critical to prevent potential cyber attacks, as well as to mitigate the harm caused by those that do occur.

One of the most common methods for sharing cybercrime information is through public-private partnerships. These partnerships involve collaboration between government agencies and private sector organizations, and allow a more comprehensive understanding of cyber threats and risks. By working together, both parties can share vital information regarding potential attacks or vulnerabilities, leading to more effective prevention and response strategies. Additionally, such collaboration often extends to ongoing investigations where real-time information sharing can enrich both parties' understanding of an attack and be used to identify the modus operandi of the actor, the root cause of the attack, or even who is behind it.

A crucial element in the fight against cybercrime is the utilization of trusted platforms and networks for the secure transmission of sensitive information among involved parties. These platforms have evolved significantly due to technological advancements and now support highly sophisticated functionalities that facilitate real-time communication and collaboration through encrypted messaging apps and secure communication channels. The incorporation of encryption not only ensures secure text exchanges but also protects voice calls from interception. This real-time encrypted communication is essential as it allows all parties to exchange information instantaneously and securely, enabling swift and effective responses to emerging cyber threats. The ability to communicate securely in real-time enhances the effectiveness of cyber defense strategies, making it possible to quickly adapt to and mitigate evolving cyber threats as they occur.

This chapter will describe the methods and limitations of cybercrime information sharing. In particular, it will illustrate the jurisdictional and classification limitations by types of crime, and the authorities for the release and sharing of related information. Guidance will also be provided concerning the documentation and qualification of information to be shared, as well as the timeliness and purposes of sharing. This chapter will provide investigators a reference framework for sharing information according to such requirements. It will also assist organizational managers in defining associated policies, systems, and procedures for defense and protection.

At the conclusion of this chapter, readers will have understanding of:

- Why should cybercrime information be shared?
- Who should share cybercrime information, both internally and externally?
- What requirements govern which type of information to share and when to share it?
- In what venues should cybercrime information be shared, and how?

Topic in Cybercrime Information Sharing

Figure 9-1 displays topic categories in the "Cybercrime Information Sharing" knowledge domain.

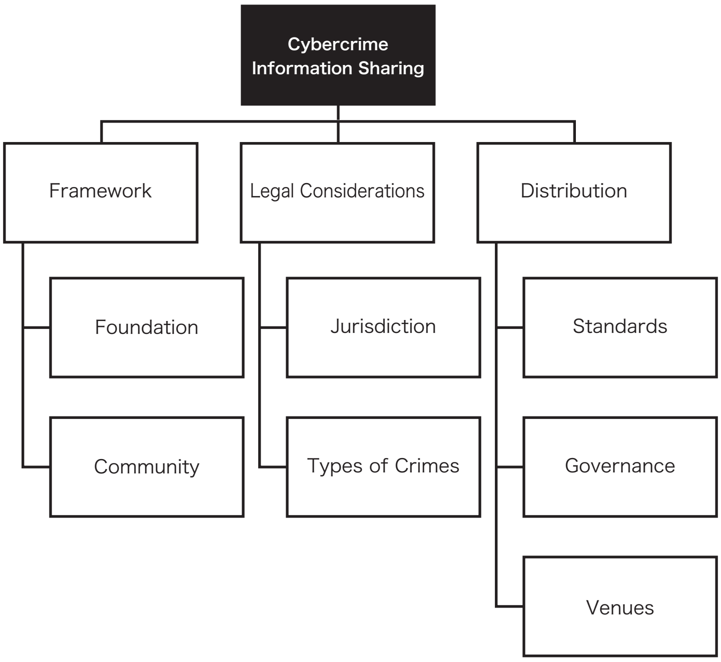


Figure 9-1. Topic Categories in the "Cybercrime Information Sharing" knowledge domain

What is Cybercrime Information Sharing?

When considering information sharing, it is important to distinguish between *information* and *evidence*. *Information* is data discovered or developed in the course of the investigation. *Information* becomes evidence when it is intended or offered to prove (or disprove) a fact or matter in a relevant civil or criminal legal proceeding. The fact that certain malware has been generally attributed to a particular threat actor[272] is useful *information*, but it doesn' t become *evidence* until it satisfies (legal and other resolution) requirements that include how the artifact relates to activities, intents, and interests of a cybercriminal or related organization. As an example, an IOC such as a signature identifying a specific malware sample is merely *information* (an artifact), and is not *evidence* unless context and impact can be established. This is a crucial realization that an experienced investigator will learn over time. Mis-attribution, based upon the reputation of an artifact rather than analysis of how it relates to a cybercrime, does not help anyone.

●Benefits and Limits:

The sharing of evidence and information developed during the investigatory process is invaluable for five major reasons:

1. Depending on the specific nature of the cybercrime committed, it can help incident response professionals or organizational defenders develop a plan or strategy for remediation, damage limitation, and recovery from the crime.
2. Information and evidence collected or developed will invariably be useful to organizational defenders in preventing future attacks.
3. Information and evidence may be useful to the larger community of defenders as they protect against attackers or remediate attacks.
4. Information and evidence may be useful in protecting the victim' s organization from civil actions.
5. Information and evidence may be useful to law enforcement in supporting a successful criminal prosecution of the attackers, if and when they are identified.

While all of the above are important reasons to share information, there are also scenarios where cybercrime information that might be helpful should not or cannot be shared or must be limited. This typically involves situations where there is intent to use the information as evidence in a prosecution, where privacy issues are involved (e.g. Personal Privileged Information or PPI), when sharing might inadvertently disclose corporate or trade secrets, and when sharing is otherwise legally enjoined. For instance, the Cybersecurity Information Sharing Act of 2015 specifically requires entities to review and remove "personal information" from threat indicators prior to sharing them.[273]

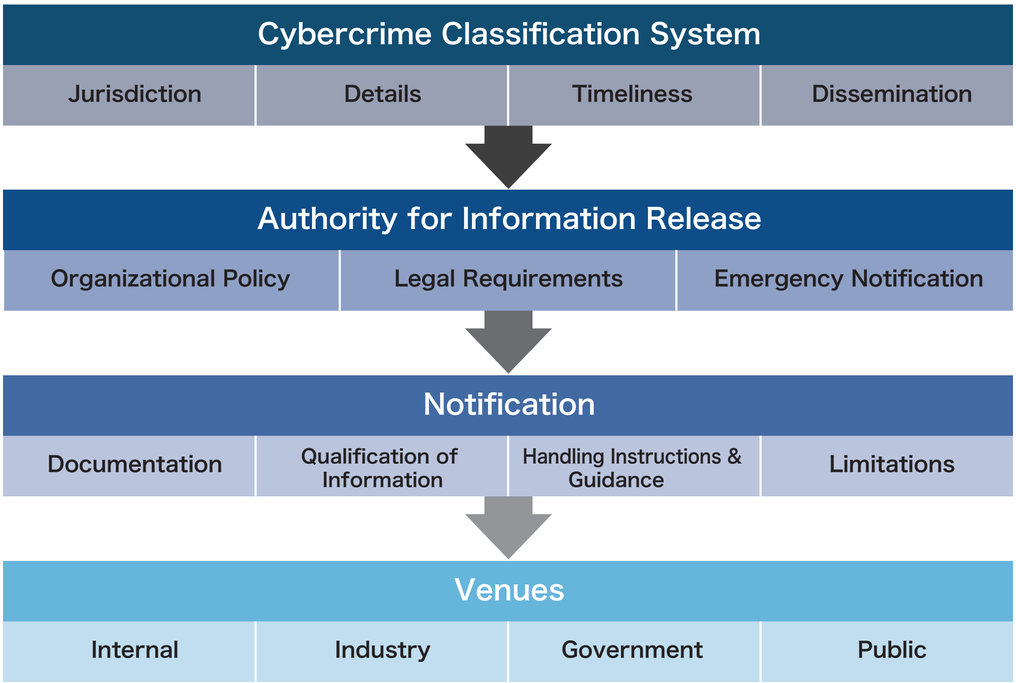
[272] http://www.threatgeek.com/2016/06/dnc_update.html

[273] https://www.congress.gov/bill/114th-congress/senate-bill/754/text - see section 104 (d)(2)(A) & (B)

Framework

In order to develop an information sharing strategy and detailed process implementation for an enterprise, one must consider both the benefits and limits of information sharing (as described above) in the context of the particular mission or business purpose of the enterprise. Every enterprise must consider the trade-offs in the context of their own unique economic utility; similar enterprises may elect dis-similar information sharing approaches as a result. The remainder of this chapter develops a reference framework for sharing information in the context of these benefits and limits. This reference framework will be useful to both cybercrime investigators and organizational managers who are responsible for defining associated policies, systems, and procedures for defense and protection.

A sample framework is described in the following model below (Figure 9-2). *Classification* of information about cybercrimes is determined by relevant jurisdictional requirements, as well as considerations of how quickly (and completely) such information sharing should be performed. The *authority* for who and how information can be released for sharing is also described. A determination of the accuracy and reliability of information to be shared is then performed to support *notification* requirements (victims, regulators, industry, etc.). Finally, the venues in which cybercrime information should be shared are detailed, including conditions for release.



Cybercrime Classification System

Jurisdiction | Details | Timeliness | Dissemination

Authority for Information Release

Organizational Policy | Legal Requirements | Emergency Notification

Notification

Documentation | Qualification of Information | Handling Instructions & Guidance | Limitations

Venues

Internal | Industry | Government | Public

Figure 9-2. Cybercrime Information Sharing Framework

The Importance of a Solid Foundation:

Cybercrime is no different than any other type of crime in that it begins with an intent or motive, as expressed by an individual or group who plans to take some action against a target or victim. The goal for cybercrime investigators is to develop evidence to prosecute where possible, and to learn from past experience to inform future preventive actions.

Although it is quite often possible to achieve preventative controls through good security practices (for examples, lock your doors and windows at night, turn on your alarm, and be alert for suspicious activity), the challenge for most enterprises is that they are managing their attack surface in the face of rapidly evolving advanced threats- cybercriminals have an asymmetric advantage over defenders. Put succinctly, given sufficient time and resources, cybercriminals are quite likely to experience some success getting into the "house".

While this obviously places a premium on robust incident response processes to "remove them from the premises", what is often overlooked (or not as well understood) is the importance of routinely recording and noting information during the course of day-to-day operations. An organization that tracks case histories and includes details such as IOCs and related activity patterns, intents, suspects, and associations creates context that can be built upon in future investigations. This is why a case management system is so important. If case management information can be systemically shared, such as via STIX/TAXII or similar methods, then intelligence can be developed to benefit the communities who participate in intelligence sharing and use.

For instance, a port-scan detected from a specific IP address 3 months ago takes on new significance when a phishing attempt is discovered from the same IP today. Case histories enable investigators or defenders to connect seemingly disparate pieces of information to enable a better understanding of motive and attribution, and to inform action. Thus, the routine collection of information about an enterprise provides the context needed to optimize investigation and resolution. *This routine collection of data forms the foundation of our information sharing framework.* In fact, the data you collect about your own enterprise as it relates to daily operations, patterns of use, and observed potential or real attacks to exploit vulnerabilities in systems and processes is the most important information you can collect and make available. Sharing this information within an enterprise is critical for effective defense. See Figure 9-3 below for a visualization of this critical case management framework:

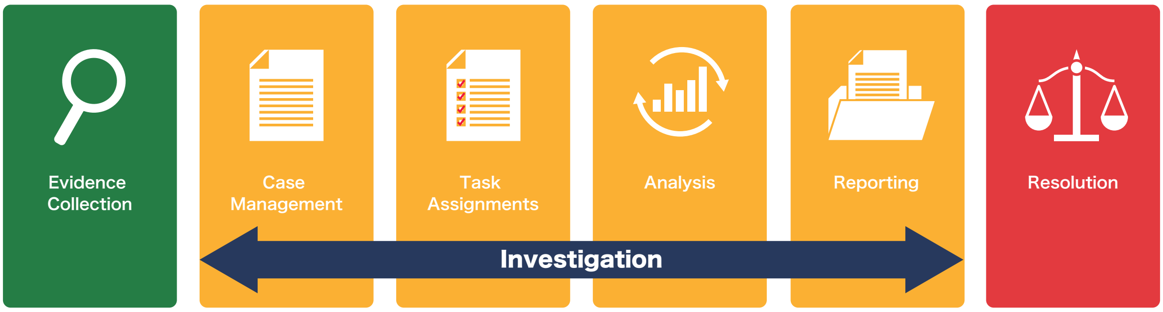


Figure 9-3. Case Management Framework

In today' s modern enterprise, this foundational information is typically collected by myriad sensors, with further context added via a robust, routine, and repeatable IR process. The information collected and evidence developed should be stored in a database accessible to investigators and defenders, with appropriate security controls. This database capability may be either internally developed or externally acquired, and the decisions about the data model, retention, storage, and accessibility constitute the trade-offs which form the first foundational layer of the information sharing framework.

Developing a Community:

After an enterprise has established a well thought out foundational layer that enables information collection and sharing within its borders, the next logical step to realize the benefits from information sharing discussed above is to share within the broader community. As long as there is adequate reciprocity, sharing cybercrime information externally has the potential to create many advantages for investigators and defenders. Because threat actors and criminals often use the same techniques and practices in an attempt to compromise multiple targets, the timely sharing of information about activities of threat actors as well as their techniques and practices can be of tremendous utility to potential community members who have not yet been attacked. The ability to share this information will be influenced by the nature of the crime and the investigatory procedures used. Leaving these more complex considerations aside for the moment, the routine reciprocal exchange of cybercrime information is typically accomplished by:

1. A policy decision stating that information collected or developed may be shared.
2. Removal or anonymization of personal information, as required by statute or regulation.
3. Removal or anonymization of sensitive information related to the corporation or government entity providing the information.
4. A decision about the appropriate forum and format in which to share the information.

Step 1 above is of critical importance, as even routine information sharing must be supported by well-understood governance policies designed to comply with relevant statutes, applicable regulatory decisions, and best business practices. Generally, data will then be anonymized as described in steps 2 and/or 3 above, with the caveat that the specifics of anonymization will be influenced by the decision in step 4 about where and how to share the information.

With respect to step 4, information may be shared in multiple formats, from relatively simple indicators of compromise (IOCs) such as a known malicious IPs, URLs, or file hashes designed primarily for use by automated security systems, up to and including detailed analytic reports designed for human consumption which identify and describe target actors, campaigns, techniques, and practices. This type of in-depth reporting, while not typically useful for blocking attacks in real-time, is critical when considering overall organizational posture and policy. If, for instance, an organization is aware of a specific campaign targeting its industry that is focused on exploiting vulnerabilities in organizational processes, it may have time to react with adjustments to the relevant process(es) and elevate awareness via focused training for its employees.

See Figure 9-4 below for a sample information sharing format framework.

Step 4 also entails deciding which venue(s) to share information with. Options include:

1. Sharing within a community developed around a particular service that the entity subscribes to. For instance, if an organization subscribes to a particular vendor' s threat intelligence, they may choose to share via that same vendor and in return receive other community members' information. This type of sharing would most typically be enabled for routine IOCs observed in IR and SOC operations
2. Sharing within a community established around a particular vertical industry sector. For example, more than 20 Information Sharing and Analysis Centers (ISACs) have been established

under the National Council of ISACs (NCI).[274] These ISACs coordinate activities within their sectors that can range from automated indicator and threat sharing to routine reporting and scheduled coordination and exchange meetings. Sharing within the ISACs is not limited to cybercrime information, as physical security threat data is also integrated into the sharing process. The integration of physical security information continues to increase in importance as the Internet of Things (IoT) expands. ISACs are also represented in the NCI by the National Cybersecurity and Communications Integration Center (NCCIC), the arm of US-CERT that responsible for coordinating recovery, mitigation, and remediation activity across the government and the private sector (especially critical infrastructure).

3. Sharing may also occur publicly with the broad community of defenders. For instance, some may choose to publish details about observed TTPs so that they can be reviewed by other investigators and defenders. Others may choose to share workflows consisting of best practices for identification, containment, investigation, and recovery for specific classes of cybercrime cases.

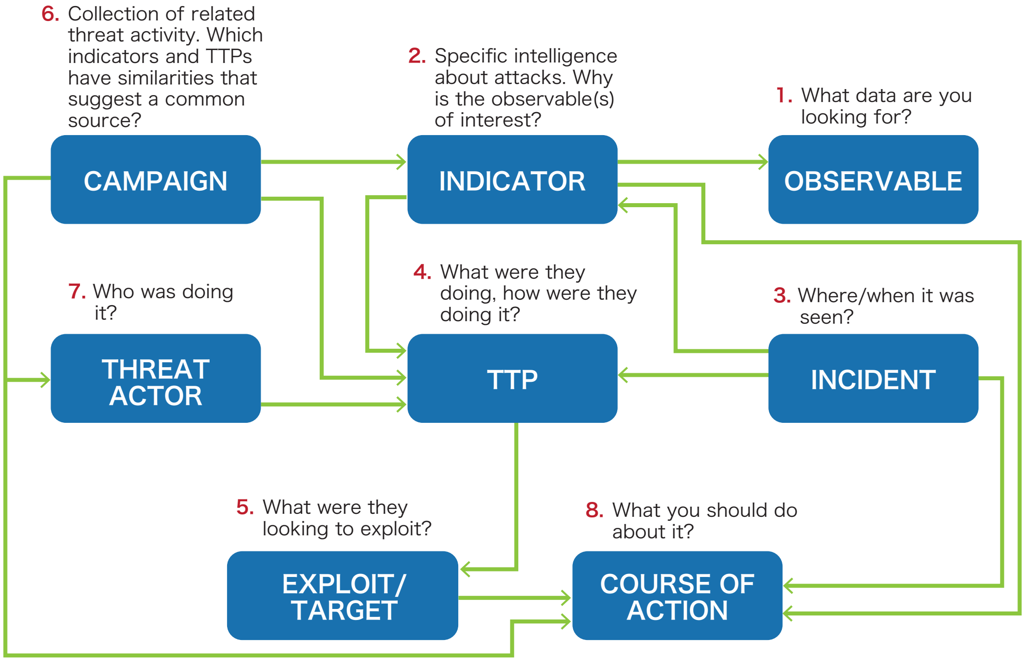

6. Collection of related threat activity. Which indicators and TTPs have similarities that suggest a common source?
2. Specific intelligence about attacks. Why is the observable(s) of interest?
1. What data are you looking for?
CAMPAIGN
INDICATOR
OBSERVABLE
7. Who was doing it?
4. What were they doing, how were they doing it?
3. Where/when it was seen?
THREAT ACTOR
TTP
INCIDENT
5. What were they looking to exploit?
8. What you should do about it?
EXPLOIT/ TARGET
COURSE OF ACTION

Figure 9-4. TAXII Sharing[275] via AIS

Legal Considerations

While there are many advantages to the timely sharing of cybercrime information broadly within the community, legal considerations must inform any sharing and give rise to some very important limitations.

[274] http://www.nationalisacs.org/member-isacs

[275] https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

Jurisdiction:

When considering sharing information related to an alleged cybercrime, the most important initial issue is determining who has jurisdiction. Without jurisdiction, a prosecutor has no authority to investigate and a court has no authority to render judgement. Jurisdiction in a criminal or civil matter is determined either by where the act was committed or where the victim was. For example, in the United States, if an act is committed in the state of Maryland, jurisdiction will fall to Maryland except in the event where a Federal law was also violated, in which case Federal courts may also have jurisdiction. While this model works well in the physical world, it presents unique challenges for crimes committed online where the victim may live in one jurisdiction, the perpetrator may live in another jurisdiction, and resources used to effect the crime- such as a computer which served malware to the victim- may be in a third jurisdiction. The fact that cybercriminals often use technical means such as anonymous proxies and header spoofing to obfuscate their true identity and location leads to further complexity in determining appropriate jurisdiction.

Determining jurisdiction is critical because it not only affects the ability to prosecute but also impacts evidentiary rules including how evidence must be collected, what evidence may be shared, who the evidence may be shared with, and how long it must be retained. It is also possible that specific details impacting jurisdiction will not be known when the investigation first begins, but will be determined as evidence is developed. For instance, a theft of corporate intellectual property may upon first glance appear to be perpetrated from Germany (based on a cursory examination of the IP addresses logged), yet in the process of the investigation additional evidence developed may in fact indicate that the true location of the perpetrator was in Russia.

The type and magnitude of the crime also may have an impact on who ultimately assumes jurisdiction, particularly at the Federal level where multiple agencies (FBI, Secret Service, DHS, ATF, FTC, SEC) each have authority under multiple statutes to claim jurisdiction depending on the specific type of crime committed. Chapter 6 contains a detailed discussion of the various types of cybercrimes such as intellectual property theft, PII theft, terrorism/national security, and ransomware/extortion.

In the U.S., the FBI and the Secret Service are the two most prominent Federal agencies. Both have broad and often overlapping jurisdiction. The FBI will typically take the lead in matters with a strong or potential nexus to terrorism, national security, and intellectual property theft. If the issue involves currency or bank fraud, the Secret Service is more likely to lead, based on broad cybercrime authorities granted by the Patriot Act of 2001.[276] Other agencies such as the Bureau of Alcohol, Tobacco and Firearms (ATF) (on matters related to arms or munitions trafficking), the Securities and Exchange Commission (SEC) (on matters related to securities law violations), or the Federal Trade Commission (FTC) (on matters related to consumer and trade fraud) will lead investigations into crimes involving related areas, but the FBI will at least support those activities.

As a practical matter, jurisdiction is often decided as much by available resources to pursue the crime as it is by statute. In addition to granting broad jurisdictional authority to the Secret Service, the Patriot Act also established Electronic Crimes Task Forces (ECTFs). ECTFs are joint-task forces comprised of local, state, and Federal agencies that pool resources and knowledge to investigate and prosecute cybercrime in almost thirty locations nationwide.[277] Pooling resources in this manner allows

[276] https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

[277] https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf

the investigative agencies to more effectively counter crimes that impact broad numbers of people or communities in multiple jurisdictions. Other countries have similar domestic arrangements and also participate with other countries when cybercrimes involve international jurisdiction issues. As described in Chapters 1 and 8, the Budapest Cybercrime Convention ("Treaty 185") and MLATs form the types of agreements that countries utilize for such investigations.

Type of crime:

The type of crime will also have an impact on what details may be shared. For example, in crimes involving theft of identity or sensitive personal information, under CISA any information shared must exclude PII of the victim, which is defined by DHS and DOJ as "personal information of a specific individual or information that identifies a specific individual".[278] Notwithstanding this guidance, there are situations where identity can be disclosed through sharing. For instance, it may be permissible to share identifying information about the source of a phishing threat, such as the originating email or IP address, even though disclosing the targeted e-mail or IP address would not be. It is also generally permissible to disclose the IP addresses used in a DDOS attack, even though doing so might in some circumstances associate the addresses with a specific individual. For many types of cybercrime, it is relatively straightforward to share useful indicators (the name or hash of a malware file, a domain or IP from which the crime originated, etc.) as well as the prevalent method(s) of infection or attack (spear-phishing, compromised USB devices, etc.) without creating a liability under CISA or other Federal privacy statutes.

If the crime involves matters of national security (such as the theft or transmission of classified information), then investigators will not typically be permitted to share classified information or evidence outside of the appropriate cleared community. In the event of IP theft, a company may choose to disclose some specifics about the type of information targeted or taken, to help alert others in the community and prevent similar attacks.

Distribution

Timeliness of sharing is also critically important, as information shared days or weeks after an attack has been detected may arrive too late to be of benefit to other defenders or investigators. For this reason and because of the sheer volume of information that may be available to share, automated methods of dissemination are preferred when possible. As discussed above, there are several mechanisms available to share threat indicators automatically through a threat exchange.

Standards

Over the last several years, standard formats and mechanisms for sharing cyber threat information have been developed and widely adopted.[279] These standards facilitate timely, actionable information sharing which can be rapidly operationalized across many enterprise environments. Figure 9-5 below

[278] https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

[279] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

shows three common standards:

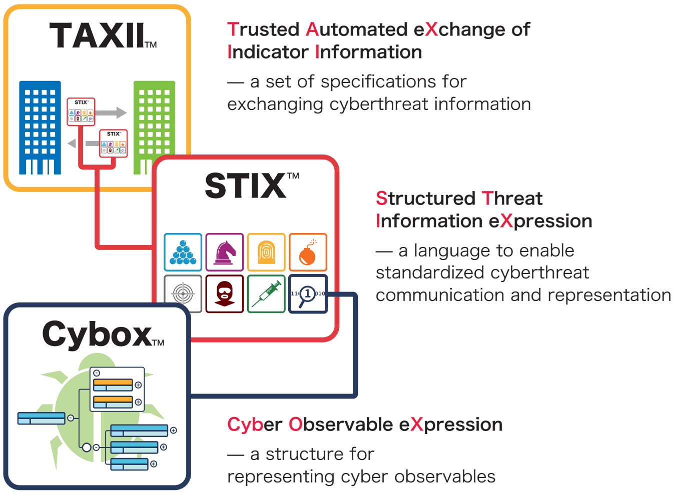

TAXII™
Trusted Automated eXchange of Indicator Information
— a set of specifications for exchanging cyberthreat information
STIX™
Structured Threat Information eXpression
— a language to enable standardized cyberthreat communication and representation
Cybox™
Cyber Observable eXpression
— a structure for representing cyber observables

Figure 9-5. Information Sharing Standards

There are situations where sharing information in an immediate manner may not be possible, either as a result of internal sanitization required as part of a legal or regulatory regime, internal review processes that protect intellectual property of the sharing organization, or merely because of the length of time it takes to completely develop the information to be shared. Another example is when sharing a vulnerability might create substantial harm. If a researcher discovers a new zero-day exploit, principles of responsible disclosure dictate that it should first be shared with the organization who owns or has responsibility for the software being exploited, to enable them to patch it prior to announcing the exploit publicly.

Governance:

The various legal limitations on information sharing related to jurisdictions, specific details that may or may not be shared, and categories of cybercrime create an environment where establishing proper governance processes for information release is critical. All organizations- public and private- should establish, document, promote, and follow a policy. A complete policy must include the following key components:

- What types information may be released
- What types of information cannot be released
- How information will be sanitized to ensure it is free from PII, IP, classified data, or anything else whose release is enjoined by statute, regulation, or policy
- Who must review the information prior to release
- What parties are authorized to receive the information
- Who is authorized to release the information
- What mechanisms will be used to disseminate the information released

It is important that the governance policy ensures compliance with key state and Federal statutes and regulations, such as:

- Electronic Communications Privacy Act of 1986 (ECPA) – regulates how communications may be intercepted, how stored information may be collected, and how non-content data (phone numbers) may be collected
- Cybersecurity Information Sharing Act of 2015 (CISA) – provides liability protection to encourage private firms to share cybersecurity information with the Federal government
- Critical Infrastructure Information Act of 2002 (CIIA)
- Cable Communications Policy Act of 1984 (CCPA) – regulates PII collected by cable providers
- Children's Online Privacy Protection Act – regulates PII collected by websites targeting children
- Gramm-Leach-Bliley Act (GLBA) – regulates financial services providers
- Family Educational Rights and Privacy Act – regulates educational institutions
- Health Insurance Portability and Accountability Act (HIPAA) - regulates healthcare providers

For private concerns, the governance policy must also ensure compliance with applicable regulations. The Federal Trade Commission (FTC) regulates private businesses and takes enforcement actions when it finds evidence of violations of data security. The FTC applies the general standard that *"a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."*[280] As of 2023, the FTC has brought 89 data security cases against private companies for failing to meet this standard.[281]

For financial concerns, the Security Exchange Commission (SEC) regulates exchanges (Regulation SCI)[282] and broker dealers (Regulation S-P)[283] to ensure the integrity of trading systems and information, and the protection of PII. The SEC can and does take enforcement action against companies that fail to meet regulatory or other standards for cybersecurity. Two prominent examples are an enforcement action against Morgan Stanley that resulted in a $1 million penalty[284] and a settlement with a financial services firm related to a PII disclosure impacting over 100,000 individuals.[285]

There may be situations where an emergency notification needs to be made in such a manner that it would abrogate the normal governance process or create a potential policy or regulatory violation. One such example would be the detection of a planned attack where going through the standard release process could result in bodily harm to an individual or group of individuals, such as an attack which would imperil critical infrastructure like a dam or an air traffic control system. In anticipation of such a situation, the governance policy for sharing and release should include an exception process that enables rapid escalation in emergency situations as well as pre-defined examples where approval may be sought concurrently or ex-post facto, such as when failure to share might reasonably be expected to result in grievous bodily harm to one or more individuals. In this situation, the goal of the governance process should be to share only the minimum information necessary to preclude the threat.

The governance process should also provide for issues and record-keeping around decisions and

[280] https://www.ftc.gov/datasecurity
[281] https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update
[282] https://www.sec.gov/spotlight/regulation-sci.shtml
[283] https://www.sec.gov/spotlight/regulation-s-p.htm
[284] https://www.sec.gov/news/pressrelease/2016-112.html
[285] https://www.sec.gov/news/pressrelease/2015-202.html

notifications as required by policy, regulation, or statute. This includes documentation and records related to when decisions were made, who made them, who was notified, and the timing of other key events. These records should be kept in an auditable format to enable demonstration of compliance for the governance process as led by an external auditor or regulatory body.

Shared information should be accompanied by an unambiguous notification that identifies the originator of the information, the intent or rationale behind the sharing, any qualifications relating to how the information was derived or how it may be used, instructions or limitations on handling the information, and how and when it must be disposed of.

For instance, the information may be perishable and after two weeks the benefits of retaining it would be outweighed by other risks relating to disclosure of sources and methods or defensive tactics. In this case, it would be possible to construct a notification that limited the time period to use the information and provided instructions for destruction or disposal. In another case, information might be classified and may only be shared with authorized entities; in some instances, the information may be intended only for a specific industry sector and shared with firms who participate in that sector' s ISAC. For automated sharing, such notifications may be scripted or pre-defined based on the use case and type of information being shared, but the notifications should still exist, be documented, and be well understood.

Venues:

No discussion of information sharing would be complete without also summarizing the venues in which information may be shared. The venues mentioned earlier provide some suggestions for US organizations, but more generally, organizations should consider communities including:

- **Internal** communities within the enterprise to support defenders and investigators. As discussed in the foundational component of the information sharing framework above, collecting and exchanging information internally is the critical foundation on which other aspects of sharing are built.
- Communities within an **industry sector**, such as one of the ISACs[286] or another ad-hoc or formal sharing organization, as covered in the discussion on communities earlier in the chapter.
- A broader **community** of defenders and investigators. Organizations can share with these communities by publishing information, indicators, and analysis broadly, whether via an automated feed through a TIP provider or a published report or blog.

Within the US government, information sharing is typically done via the Department of Homeland Security (DHS). One such DHS program is automated indicator sharing, or AIS[287]. The AIS program provides for “machine speed indicator sharing” using the aforementioned STIX and TAXII standards. Entities sharing information using the AIS program in accordance with the guidelines for PII minimization and protection are afforded certain key liability protections, especially related to the disclosure of PII and regulatory actions the government might initiate as a result of the information shared. See Figure 9-6 below:

[286] http://www.nationalisacs.org/member-isacs

[287] https://www.dhs.gov/ais

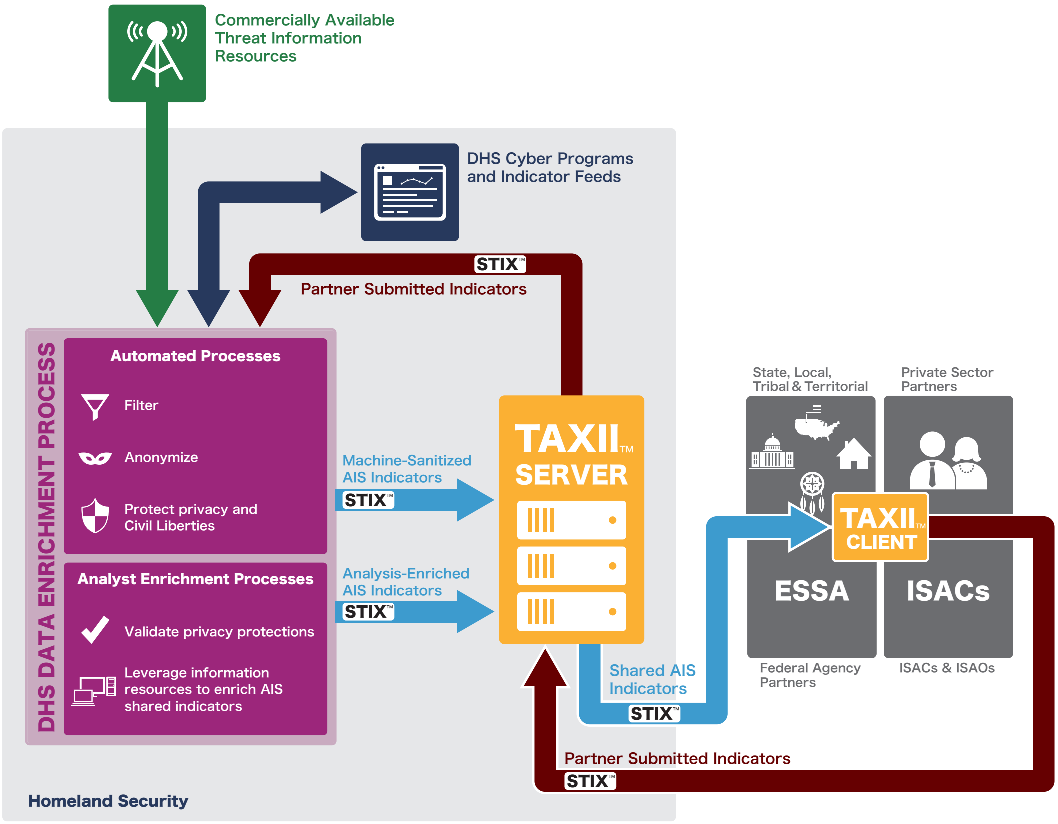


Figure 9-6. US Venues

As previously described, the execution framework of the CIBOK Taxonomy details the interrelationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon determination of the type, available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

Chapter 9: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the types of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

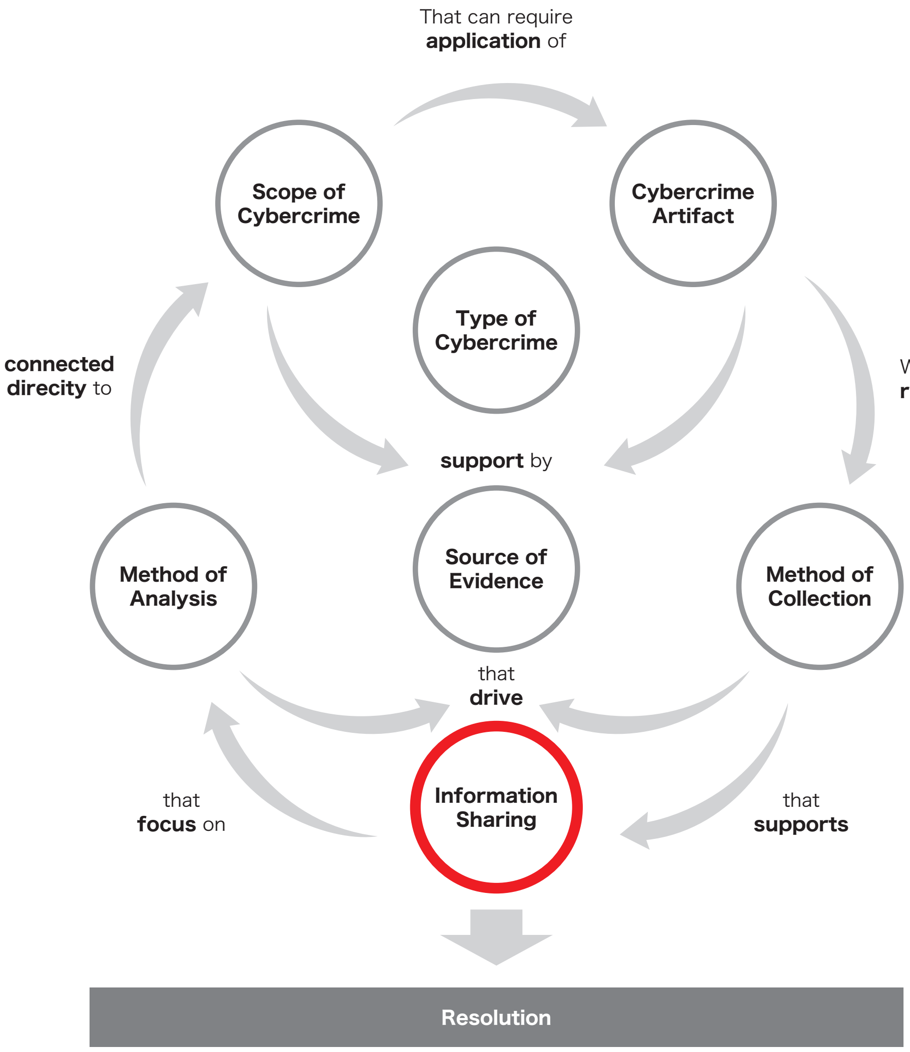


Figure 9-7. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 9-8. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 9-9. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should govern the information to be shared and the methods of dissemination/distribution.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. Intelligence should collect but not distribute information except as specified by organizational policies.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigators should collect and analyze information but only share according to organizational policies.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will provide restrictions and penalties for the sharing of information. This will assist the judiciary in defining policies for investigators and intelligence functions, and to inform executive staff of requirements.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The scope of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when, according to which organization/functions/personnel are affected. Public relations must coordinate with the judiciary to ensure effective communication with appropriate external agencies, according to legal limitations.

Support – require procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 9: Review

1. Why should cybercrime information be shared?

   Answer: To help other investigators inside and outside of an organization and increase knowledge

   Examples: An organization experiencing an attack can benefit from another who experienced similar TTPs or reflected IOCs

2. Who should share cybercrime information internally and externally?

   Answer: Only those with authority to do so

   Examples: Depends on RACI, but generally the Judiciary and Public Relations

3. What requirements govern which type of information to share and when to share it?

   Answer: Standards and Governance

   Examples: STIX/TAXII/CybOX, GLBA, HIPAA, etc.

4. How should cybercrime information be shared, and in what venues?

   Answer: Internally, Industry Sector, Community

   Examples: Other functions of an organization, ISAC' s, OSINT/PROPINT forums

Case Study 9: Mobile Application Payment Fraud

- **Crime**: Information (Identity) Theft and Fraud
- **Suspect(s):** Access broker and small group of individuals
- **Means**: Social engineering, phishing, exposed credentials, and malware (infostealers)
- **Motive**: To commit fraud
- **Opportunity**: Facilitated by insufficient security measures (including inadequate security awareness regarding phishing, poor password hygiene, and weak identity verification) leading to compromised email accounts and user credentials

In 2024, an investigator received a request from a law enforcement agency to assist with a fraud case affecting a global company’ s mobile payment application customers. Victims' credentials had been stolen and used to make unauthorized payments through the mobile payment application. Some of the payments had been made in person, but attackers had also made fraudulent purchases which were shipped to U.S. postal addresses.

In the course of the investigation, research and the utilization of advanced attribution and analytical techniques were used, and various tools and enhanced open-source intelligence (OSINT) were leveraged. The results of the investigation are detailed below.

●Initial Data Collection and Sharing

The initial information provided by the law enforcement agency included compromised email accounts, suspicious IP addresses, and details of unauthorized transactions. This data was shared with the investigator following a structured incident response (IR) process, ensuring proper chain of custody and enabling accurate analysis.

●Collaboration with External Sources

The investigator then accessed data breach databases and threat intelligence tools which were part of the existing partnership between the law enforcement agency, the global company, and the investigator. These sources provided additional context and corroboration for the compromised credentials and IP addresses.

●Utilizing Established Frameworks

The investigation followed the Cybercrime Information Sharing Framework (CISF), which emphasizes the importance of timely and secure information sharing. This framework helped the investigator collect, analyze, and disseminate information effectively.

●Anonymization and Compliance

Personal Identifiable Information (PII) and sensitive corporate data were anonymized before sharing to comply with legal and regulatory requirements, such as the Cybersecurity Information Sharing Act (CISA) of 2015. This ensured that shared data did not compromise privacy or intellectual property.

●Secure Communication Channels

The investigator used encrypted messaging apps and secure communication channels to exchange information with the law enforcement agency and the global company. Real-time, encrypted communication was essential for swift and effective responses to the emerging threats.

●Real-Time Information Sharing

Similarly, the investigator shared real-time updates and findings with the global company's security team, enabling them to quickly adapt defensive strategies to meet relevant threats. In some cases, a secure real-time line of communication was established using secure messaging apps to ensure the confidentiality and integrity of the information being exchanged. Shared information included Indicators of Compromise (IOCs) such as malicious IPs and email addresses used in phishing attacks.

●Research methodology

After receiving information provided by the global company, the investigator conducted searches across various sources to analyze compromised emails, devices, and IP addresses. Each found result underwent a complete analysis, as if it were original data provided by the client. Consulted sources included:

- **Data Breach Databases**: Multiple exposures of the analyzed emails alongside plaintext passwords were detected, enabling total control over accounts if passwords had not been updated or were being shared between services. Further analysis revealed that the Badoo breach (first discovered in 2016) was a common reference point among all exposed accounts.
- **OSINT Tools**: Social networks were associated with the phishing attack email, which was identified as belonging to a marketing and advertising professional in the USA.
- **Threat Intelligence Tools**: Malicious activity and suspicious high traffic were detected from some of the IP addresses used for the attack, indicating possible contact with malware.

●Investigation Summary

Subsequent analysis revealed how the attackers gained control of the global company's customers' email accounts through breaches and infostealer families which infected users' devices. Using hijacked email accounts, the attackers then accessed the clients' payment platforms to carry out fraudulent transactions by resetting passwords and PINs for the global company's application, sending reset emails to the compromised email accounts.

In addition to leveraging breaches and infostealers, the attackers had launched a phishing campaign to complement the attack and target more victims by contacting the global company's clients via email and requesting personal credential information (ID and PIN used on the global company's platform). Using the list of compromised accounts, the attackers ultimately accessed the global company's platform from various devices, alternating between accounts with bank details to make fraudulent payments.

The investigator determined that the attack appeared to be perpetrated by a small group based on evidence of multiple mobile devices used for fraudulent operations. This information could be confirmed with security camera images or video from locations where payments were physically made. It is also possible that an additional criminal (or criminals) was guiding the technical operations remotely without appearing at the physical locations where fraud was committed.

●Conclusion and Recommendations

The investigation revealed that the fraud had been enabled by customer devices infected with infostealers (via social engineering) that stole email credentials, granting attackers repeated access. To mitigate this risk, it was recommended that customers remove the malware from their compromised devices and change passwords for both their email and payment platforms. Additionally, the implementation of two-factor authentication (2FA) for email and the global company's application was advised to link usage exclusively to clients' mobile devices.

Following the NIST 800-63 directive, the investigator also advised the implementation of additional security validations to check password exposure for new users or password changes, preventing the use of previously exposed passwords.

Chapter 10

Management Framework

Introduction

Every organization, whether public or private, has limited resources to support functions and related procedures. Those resources must be managed for efficiency of scale and scope of application. Incident response, investigation, and resolution of cybercrimes is a relatively new activity for organizations that has not heretofore been organized as a common function (as compared to finance, administration, information services, or customer support).

Cybersecurity as an organizational function is a relatively new component. The executive function is matrixed to multiple strategic organizational functions including legal, IT, and administrative; and operational capabilities are negotiated between shared services functions such as IT and administration, and business units and their respective functional requirements versus regulatory mandates.

As the recognition of cybercrimes and their impacts on business continuity, both directly in operations as well as indirectly in market performance, has grown since 2013, the need for higher visibility and defense strategies (both active and passive) has correspondingly evolved. This has brought changes to first and third party cybersecurity management structures, strategies, and related tools. Security Operations Centers, cyber contingency management plans, and cyber incident response plans have become industry mandates with Board-level accountability. There is a growing need for cybercrime investigative functions to be integrated into organizations' risk management functions to ensure alignment with business priorities.

This chapter will articulate the structure and framework for constituting, planning, and executing a management framework for the cyber investigations function. Just as information services have expanded to support every organizational function and management frameworks have evolved, crimes committed with cyber tools or facilitated by cyber TTP' s are a new dimension for organizations to investigate and defend against, and define with associated procedures and tools. Descriptions of hierarchical and matrixed organizational structures will be associated with the activities performed by the cyber investigations function and personnel. In addition, to bridge the gap between technology and business, the cybercrime investigations function will be integrated with risk management best practices.

This chapter will provide investigators with a reference framework for developing effective methods of evidence collection according to such requirements. This will also assist organizational managers to define associated policies, systems, and procedures for defense and protection.

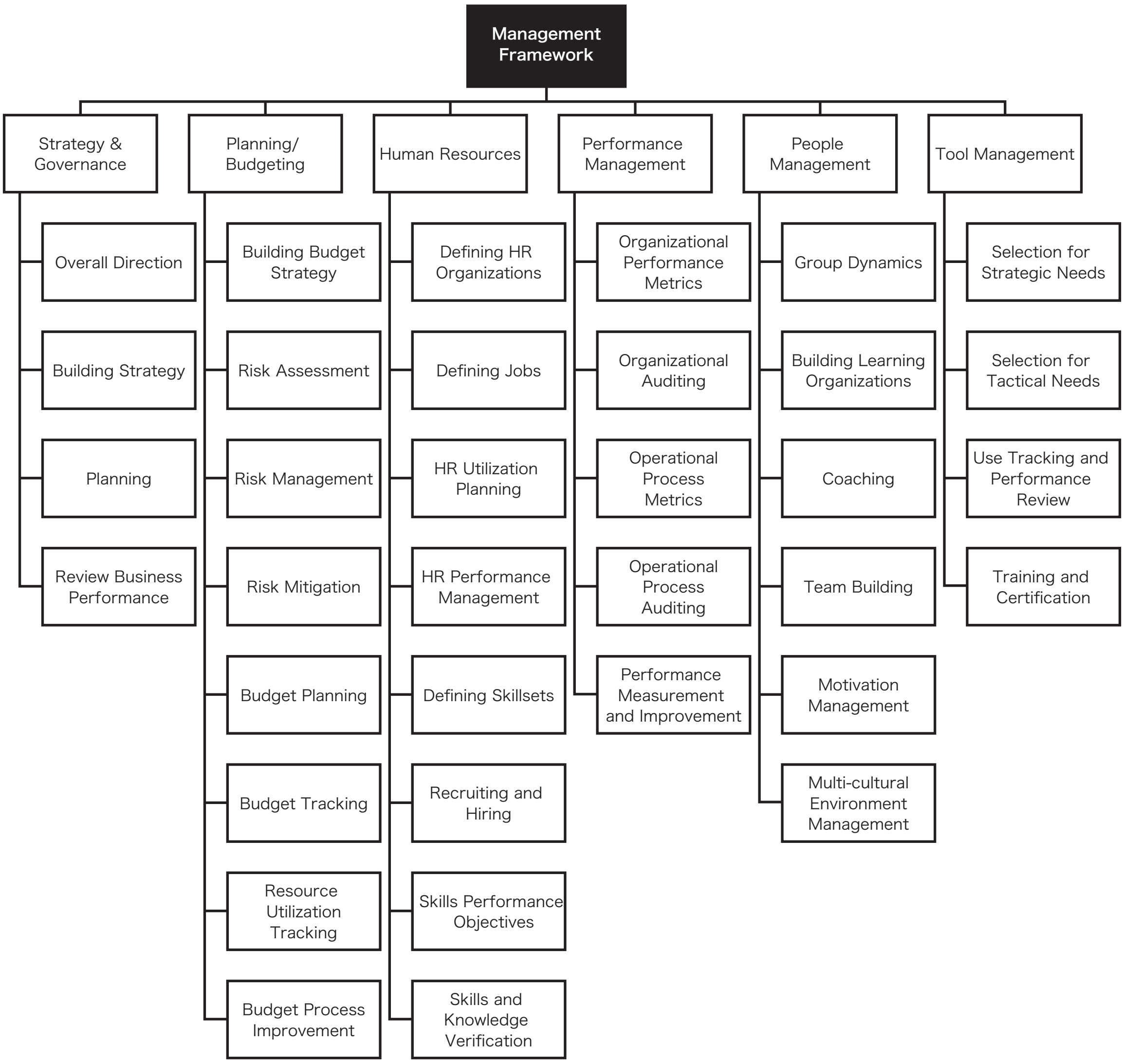
At the conclusion of this chapter, readers will have understanding of:

- What is the purpose of a cybercrime investigation and resolution function?
- How should the function be organized and managed?
- What is the strategic objective of that function?
- How should the CI function relate to governance and management functions?
- What are the resource requirements (staff, tools, and community) of that function?
- What are the technical and experiential requirements to staff, manage, and lead/govern that function?

- How should the function' s (and related staff' s) performance be measured?
- What organizational communications and strategic involvement, and in which organizational channels, should be implemented for success?
- Which organizational executive function(s) should the cybercrime investigations and resolution function report to?

Topic in Management Framework

The following figure displays topic categories in the “Management Framework” knowledge domain.



Management Framework
Strategy & Governance
Overall Direction
Building Strategy
Planning
Review Business Performance
Planning/ Budgeting
Building Budget Strategy
Risk Assessment
Risk Management
Risk Mitigation
Budget Planning
Budget Tracking
Resource Utilization Tracking
Budget Process Improvement
Human Resources
Defining HR Organizations
Defining Jobs
HR Utilization Planning
HR Performance Management
Defining Skillsets
Recruiting and Hiring
Skills Performance Objectives
Skills and Knowledge Verification
Performance Management
Organizational Performance Metrics
Organizational Auditing
Operational Process Metrics
Operational Process Auditing
Performance Measurement and Improvement
People Management
Group Dynamics
Building Learning Organizations
Coaching
Team Building
Motivation Management
Multi-cultural Environment Management
Tool Management
Selection for Strategic Needs
Selection for Tactical Needs
Use Tracking and Performance Review
Training and Certification

Figure 10-1. Topic Categories in the “Management Framework” knowledge domain

What is the Cybercrime Investigations Management Framework?

It is critical to understand the conflicting elements confronting corporate organizations with regards to managing reputational risk, legal notification requirements, and the relatively new "threat information sharing" directives. These represent real and driving forces for most corporations today and understanding these requirements will assist in improving the velocity of cybercrime investigations - whether public or private.

As mentioned, cyber incident response and investigation are not new activities, but the increased governmental oversight via mandatory reporting requirements and/or financial penalties related to breaches of privacy[288] has elevated the importance of proper planning and management of investigations functions because of the potential liabilities. Another compounding element is the recent private sector cybersecurity information sharing directives[289] that acknowledge the investigative intelligence contained within organizations related to both historic and on-going criminal cyber activities. A further complicating factor is the evolution of cybercrime as a service (CaaS). For example, when highly skilled criminals exchange goods and services through the dark web to commit crimes, a traditional technology-oriented IT security management and incident investigation framework is insufficient. It is no longer possible to consider appropriate resource allocation and effective response by focusing solely on the what and how; instead, the purposes, motives, and objectives of crimes must be investigated by focusing on who and why, informed by visibility into the background of the crime or breach.

This newly evaluated role of cyber security incident response and investigations fused with elements of cybercrime resolution is a relatively new activity for organizations that has not heretofore been organized as a common function (as compared to finance, administration, information services, or customer support). Cyber security and cybercrime investigations share many common technical and procedural methods, tools, and training. However, the same is not necessarily true when it comes to management functions and objectives, as cyber security is a support function of IT and MIS which in turn support business functions with a primary goal of business continuity and information protection. Cyber investigations primarily support risk management and have specific intelligence and evidence development and management procedures that differ significantly from IT procedures.

While there are many existing cybersecurity frameworks and guidelines that effectively address evolving cyber threats, implementing all suggested countermeasures and controls would require massive financial and human resources, and it would be very difficult to prove their effectiveness to boards and executive leaders. It is therefore critical to ensure an alignment of risk profiles and priorities around business strategies among business leaders, stakeholders, security departments, and cyber investigation functions. Underlying this discussion is the need to establish a common understanding of what needs to be protected in an organization. Without this understanding, poorly-aligned and dispersed measures and initiatives strain an organization' s resources and require greater investment and recruitment. The inappropriate allocation of resources to manage risk is far too

[288] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC and http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

[289] https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

common, creating cybercrime investigative functions that do not classify or track the most critical key performance indicators (KPI' s)- leading to impacts including poor asset, data posture, and identity hygiene management.

The cybercrime investigations management framework addresses all of these challenges by clarifying the purpose, role, scope, and objectives of the cybercrime investigations function.

Strategy & Governance

To be included in strategic capabilities as a function of an organization, the purpose of cyber investigations must be understood. Strategy requires a definition of the CI function, its utility, how it should be organized, and a responsible structure. Cybercrime investigations are simply a security or IT function.

Overall direction (e.g. vision, mission, or purpose)

The purpose of the Cyber Investigation (CI) function is to utilize a root cause analysis framework[290] to assist decision makers with understanding the requirements of investigating crimes committed by cyber actors, or facilitated by cyber tools, in order to plan and equip an organization with necessary risk awareness policies and training (and requisite tools, staffing, and support) to prevent or manage those risks.

To position CI as a strategic function and incorporate it into the organizational roles, organizations must define targets to be protected (its management scope and risk scenarios) in line with business needs and strategies, assets owned, and values provided. Clarifying targets to be protected specifies the purpose of the CI function, and dictates an efficient structure and methodology to fulfill assigned responsibilities.

The importance of governance in the private sector has already led many companies to implement a cybersecurity management system integrated with senior management layers including Boards of Directors. In addition, the World Economic Forum (WEF), in cooperation with the National Association of Corporate Directors and the Internet Security Alliance, created the Cyber Risk Board Governance Principles to help companies become more resilient against cybercrime. A consensus has formed that cyber risk management should be treated as a management issue- a trend that is expected to intensify in the future, requiring the CI function in the private sector to be further aligned.

The vision the CI function should project to the organization' s staff and decision makers is one of competence from experience and professional knowledge in the performance of their work supporting that function. In private organizations, the CI vision must be based on management and business strategies. The mission of the CI function is ultimately to reduce risks of business interruption, and coincidentally to resolve incidents with remedial actions that will prevent future recurrence through deterrence or corrective actions (including policy, procedures, training, and technical capabilities). Organizations have limited resources to fulfill their missions and visions. Before developing a strategy for the CI function, it is necessary to understand cyber and technology risks that align with business

[290] https://en.wikipedia.org/wiki/Root_cause_analysis

management and strategy. This enables an understanding of cybercriminal targets and objectives, ensuring efficient and meaningful resource allocations that consider business priorities and integrate the CI function with business risk management activities.

Building Strategy

To achieve the described objectives (vision, mission, and purpose), an organization needs to align the CI function across risk management, information security, and legal– to identify crimes through assessment, investigate them through (jurisdictional and organizational) accepted procedures, and resolve them through technical and organizational policies and remediation efforts. This requires strategic planning and development of the CI function.

Such strategic activities and imperatives of the necessary efforts are described in a planning commission called "GLACY" (Global Action on Cybercrime/ *Action globale sur la cybercriminalite*)[291] which was funded as a research and development effort by the European Union and the Council of Europe in 2013. In a related project report "Law Enforcement Training Strategy Project area specific strategies"[292], the results expected of the project included strategic objectives to address:

- Engagement of decision-makers
- Harmonization of legislation
- Judicial training
- Law enforcement capacities
- International cooperation
- Information sharing
- Assessment of progress

Although defined for public policies and governmental/law enforcement direction, those objectives can also be generally applied to private sector organizations as well with a simple translation in business terms as:

- Engagement of decision-makers
- Awareness through training and communication of cyber risks
- Organizational cyber risk management policies and procedures development
- Staffing, training, and equipping CI and risk management personnel
- Measuring organizational and CI functional performance
- Industry and Law Enforcement information sharing
- Auditing and continuous improvement

These objectives can lead to beneficial outcomes including:

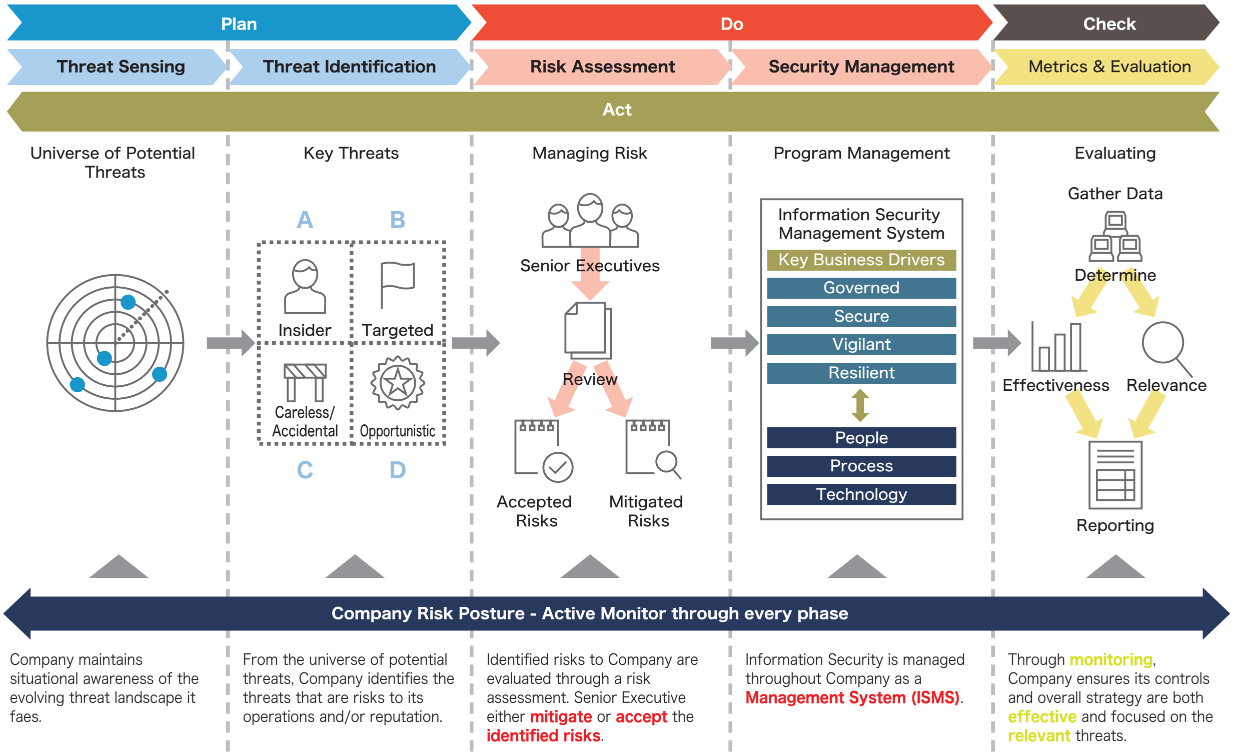
- Introduction of new technology to meet business needs
- Elimination of initiatives not producing value

[291] http://www.coe.int/cybercrime

[292] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168030287b

- Enhanced value of existing IT and security investments, including optimized IT architecture and improved observability
- Improved visibility around resource utilization
- Optimized personnel structure

Building organizational strategy for the CI function requires communication so that traditional business functions can be adapted to incorporate the risk mitigations offered by an awareness of cyber risks (as mentioned in previous chapters) and remediation through investigation and resolution. Cyber risks are commonly perceived situationally and strategic organizational functions are often misaligned through the emergency allocation of resources to competing sources. Accordingly, it is useful to have a reference framework for understanding the objectives of cyber incident response, through resolutions that the CI function should be constructed to perform. The activities, including the focus objectives of each activity in sequence, are described in the following figure.



Company maintains situational awareness of the evolving threat landscape it faes.

From the universe of potential threats, Company identifies the threats that are risks to its operations and/or reputation.

Identified risks to Company are evaluated through a risk assessment. Senior Executive either **mitigate** or **accept** the **identified risks**.

Information Security is managed throughout Company as a **Management System (ISMS)**.

Through **monitoring**, Company ensures its controls and overall strategy are both **effective** and focused on the **relevant** threats.

Figure 10-2. CI PDCA Process

As depicted in the preceding figure, the CI function has different goals in support of a strategic risk management function to Plan, Do, Check, and Act (PDCA) upon the organization's cyber risk awareness and incidents. The figure does not represent the CI function's activities as static, but rather as a continuous improvement process to support the strategic objectives of the organization as a whole. Within those activities, different organizational elements must be included for cooperative achievement of the risk management objectives. The CI function should be planned as a PCDA component of an organization, but it will operate as an Observe, Orient, Decide, and Act (OODA) continuous loop. That model[293] was originally created for military purposes but has been adapted for

[293] http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html

business strategy purposes in many guises. As applied to cyber investigations, it can be contextualized in common IT/IS vernacular as Detect, Respond, Remediate, and Improve as seen below.

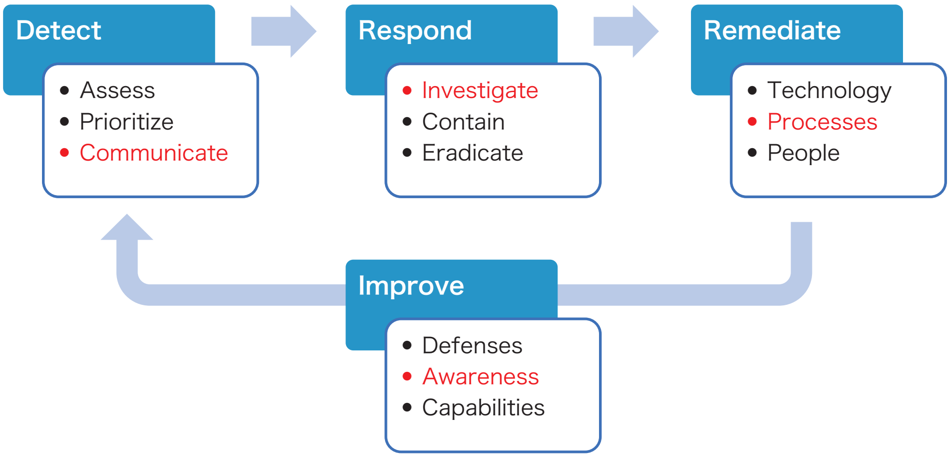


Figure 10-3. CI OODA Loop Process

●Detect

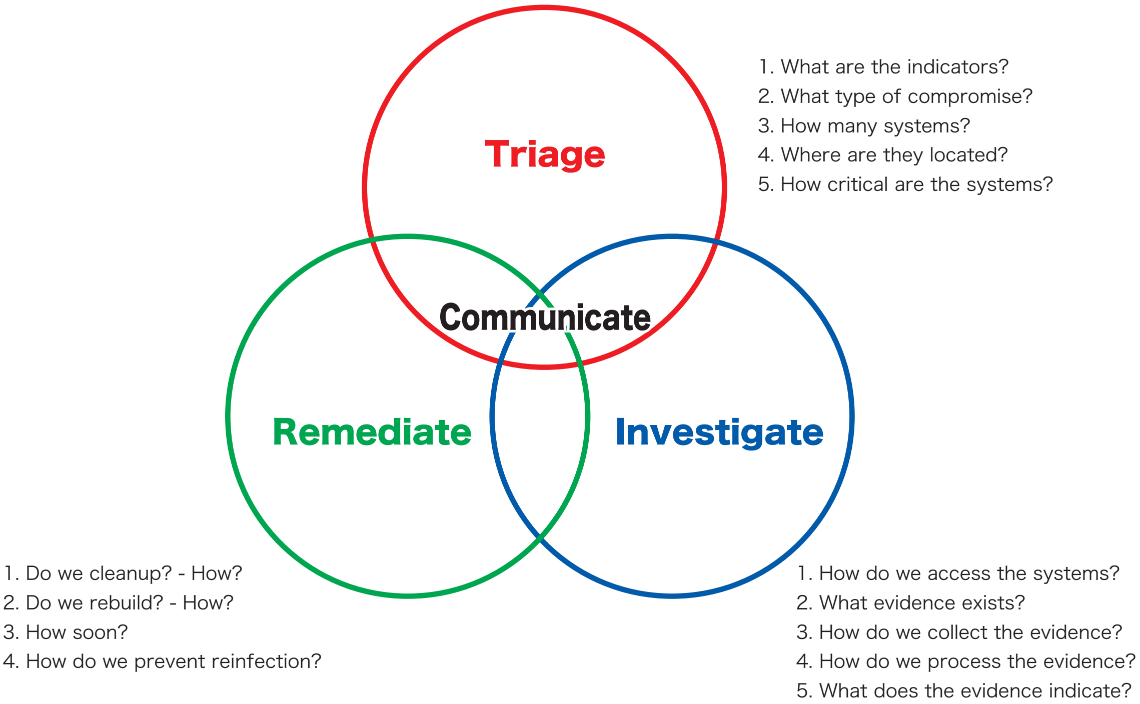
In the Detect goal, the CI function must involve organizational decision makers through communication,helping them appreciate the nature of the risk by its category (information theft, sabotage, extortion, theft, defamation, etc.) and its scope of impact (money, operations, employees, corporate brand, etc.) on the organization. For example, a “banker Trojan” discovered through SIEM alerts concerning malicious communications with a known botnet address that is determined (through investigation) to be installed on an IT support user’ s computer, represents a different risk (and corresponding allocation of organizational resources) than if the malware were installed on a financial controller’ s computer[294]. As such, the assessed risk can be prioritized by the evidence in the detection – and communicated to executive functions for appropriate response according to organization’ s policies and procedures. This is an example of risk assessment- while the Trojan is the same malware in both instances, the nature of the risk and appropriate response differs based on its unique context.

●Respond

In the Respond goal, the CI function must make decisions about how to contain or eradicate the cyber risk(s) – determined through investigation to fully appreciate the nature, scope, and impact of the risk. For example, Law Enforcement may request that an organization not eradicate a detected backdoor Trojan or bot enlistment tool until they have collected necessary evidence to support their investigation objectives (or an organization may wish to understand the intent of a malicious intrusion in order to better recognize weaknesses in their architecture or policies). In such cases it is still necessary to contain the risk to a manageable impact – but the decision to pursue containment or eradication crucially depends upon an effective investigation to inform the subsequent activities. As described in previous chapters, the response activity includes collecting information through assessment and investigation to inform decisions about resource requirements and allocations. The

[294] This is not to say that a banker Trojan on any organizational system cannot be used to pivot to other high-interest/risk computers in the organization, of course. This is simply an example of risk evaluation for communication.

following figure provides related context.



1. What are the indicators?
2. What type of compromise?
3. How many systems?
4. Where are they located?
5. How critical are the systems?

1. Do we cleanup? - How?
2. Do we rebuild? - How?
3. How soon?
4. How do we prevent reinfection?

1. How do we access the systems?
2. What evidence exists?
3. How do we collect the evidence?
4. How do we process the evidence?
5. What does the evidence indicate?

Figure 10-4. Cyber Incident Response activities and decisions

●Remediate

In the Remediate goal, processes take precedence over human factors (people) or technical solutions. For example, simply eradicating a malicious Worm from one computer based upon an IOC that leads to that single computer may not be enough. The Worm can take various forms and perform malicious operations within the network. Therefore, it may be more effective to remove not only the Worm itself, but also any associated malware, from all computers based upon properties that identify the Worm (without looking for matching IOC’ s). A process that includes adaptive thinking and tools will support effective detection and response activities that enable efficient remediation of cyber risks.

All too often, organizations rely upon tools to remediate detected cyber incidents and risks. This approach works well as long as the tool in question is configured correctly and is actually capable of detecting the threat in the first place. This “Vendor Dilemma” is a concept that has been developed over the last ten years through work on increasingly complex cybercrimes. Essentially, the dilemma shares experiences with epidemiology – when a new virus is discovered, its impact to the initially infected population can be devastating. However, once scientists can acquire samples and have the necessary time to analyze them, a reasonable vaccination can often be developed. The period of time between the index case and when the vaccination is available represents the most critical and dangerous period to the masses.

Applying this concept to incident response, investigations, and cybercrime resolution presents a harsh reality. Strict reliance on vendor tools will only detect or protect you against yesterday's threats. Cyber adversaries know vendor tools as well as, if not better, than cyber investigators and incident responders. The effect of this knowledge is that adversaries will try to develop their attacks such that vendor tools do not detect their TTP’ s.

Tools meant to protect an organization are only as good as the people who use them, and are limited by the configuration (and capabilities/suitability) of tools to requirements. As an example, antivirus is a commonly-used and relied upon tool for detecting and remediating malware in organizations and individual computers. Antivirus, and even “next generation antimalware” and EDR tools, require updates and patches – to the service as well as related definition files for signatures, policies, or models that they employ, or to explicit rules that may be defined for specific remediation tasks from time to time.

If the antivirus agent is not configured properly on the host computer, is not updated/patched consistently with other hosts, or does not have accurate and consistent definition files, that tool will actually create a cyber risk that can be exploited either intentionally or simply by evasion- enabled by the reliance of the organization (on the inadequate remedial tool to their needs) and the inability of the tool to serve its designed purpose.

This is easily seen and understood within the antivirus community. Adversaries are constantly modifying and manipulating malware to defeat the detection capabilities of antivirus tools. In addition, adversaries are using popular sites like VirusTotal to conduct monitoring exercises to determine whether their unique malware has been manually detected. This limitation does not just reside within the antivirus community and is shared across a wide range of technologies like IDS, IPS, etc. Here is where the dilemma begins– despite the weaknesses identified with vendor tools and the fact that adversaries are likely testing and tuning their attacks against the very tools you are relying on for protecting your environments, you could never do without them.

Sometimes personnel have not had the opportunity, training, or experience to understand the full capabilities or limitations of vendor tools, or non-vendor skills or processes to manually examine data elements. In particular, a lack of understanding around how to handle evidence, priorities, and appropriate procedures and responses can lead to fatal errors and corruption of the evidence trail. This presents another type of “cyber risk” if they are tasked with management of cyber risks. Accordingly, processes for effective tool selection and implementation/management, the recruiting of skilled personnel, and associated training and performance assessments to develop critical remediation capabilities to cyber risks in the CI function are interdependencies of related remediation processes. The processes, though, should define the remediation.

●Improve

Every effective strategy involves a continuous improvement goal. A major enabler for continuous improvement goals is a cross functional group with varied expertise outside of the CI core area. Without learning from mistakes (and successes) of the past, an organization cannot effectively plan for future objectives. This applies to the CI function. The Improve goal supports the development and execution of strategy by increasing awareness. Awareness is a coincidental activity to improving defenses and capabilities of the organization. Awareness can be a result of incident investigations and related technical remediation, but when it is used to improve technical defenses and personnel training it becomes a strategic support activity that helps evolve the CI function. For example, the visualization of security posture (which includes an organization’ s cyber hygiene and threat hunting activity) can assist in setting improvement targets via numerical goals; when it is used to improve technical defenses and personnel training, it also strategically supports the CI function. The utilization of the cross functional group described above helps to accelerate broader adoption because the working products of this effort are published not in the singular voice of CI, but rather with risk, IT, legal, and other common business languages.

As incidents are detected, investigated, and remediated, and the improvement of organizational capabilities is achieved, results should be systematically utilized as a feedback loop to help improve new detections and other aspects of investigation. That feedback loop ensures continuous improvement.

Planning

Planning for the CI function of an organization depends upon the goals and objectives described by mission and objectives as defined by strategic organizational elements. Generally, any organizational planning requires four major functions as described in the following table.

Figure 10-5. Planning for the CI function

Function	Description	Activities
Planning	Look to the future	Create a detailed action plan aimed at some organizational goal
Organizing	Structure for success	Determine resource allocations and organization
Leading	Show how it is done	Connect with staff by communicating, motivating, inspiring, and developing towards higher productivity
Controlling	Learn and improve	Evaluate performance for improvement

These core activities describe the role of the function and management of cyber investigations. Planning provides a decision framework for determining goals, and methods to achieve them by organizing limited resources and allocating them efficiently and effectively. Leadership is demonstrated, not taught academically. Particularly in a highly technical activity (as CI necessarily is), leadership is best “shown” through example – not managed from an office. Managing is an important activity, of course, and any expenditure of organizational resources (time, personnel, money, or technology) requires accountability – which will be described in context later in this chapter. Leadership, though, involves helping staff develop and evolve their own skills and knowledge. Learning from past performance helps an organization evolve through its requisite functions.

Review Business Performance

The effectiveness of any organizational capability is measured by an objective assessment of performance in the following areas: (1) core activities, (2) adaptability to accommodate additional requirements, (3) efficiency of skills and financial resource employment, (4) comparative assessment of the same to similar resource functions of the organization, (5) historical pace of change and correlated rate of policy/procedure/staff changes, and (6) confidence in CI leadership (top-down as well as bottom-up) by the organization.

1. Core activities of the CI function include the previously described goals of detect, respond, remediate, and improve. These elements need to be translated in a business impact statement that describes a measurable value like “Return on Investment” or “Value of Investment”.

2. Additional requirements or short-term goals may arise according to case requirements, and a high-performing organization will be adaptable in their processes and skills to facilitate changes as needed.

3. As procedures and skills improve through team organization and employment of “best practices” (both external and internal), efficiencies of scale and scope will emerge.

4. Every technical function can be compared to similar objective criteria in other skills-based functions of an organization. Such comparative performance analysis is useful to determine a measurement baseline or a set of criteria for differential analysis (sometimes both) to improve organizational functions.

5. Highly technical environments require aggressive skills and tools development through training and the recruitment of new skilled workers. Performance improvements as a group or function are achieved with correlated changes in procedures that keep pace with technical skill evolution; however, change should be managed responsibly.

6. Performance is ultimately a reflection of the confidence that an organization has in the function’s leader(s). A leader who demonstrates sound technical skills and knowledge from experience will be highly regarded by staff; similarly, a leader who demonstrates efficient resource utility and success around strategic goals will be highly regarded by executive management.

Planning/Budgeting

No function of an organization can exist without a source of funding and a plan for cost and resource allocations. Cyber investigations have historically brought operating costs that an organization suffers incidentally in the normal course of operations. A well-planned organizational function, however, can alleviate many of the incidental costs with budget planning and managed execution for requisite facilities, equipment (including software), strategic vendor agreements, and personnel.

Building Budgets Strategy

The CI function as a highly technical organizational capability requires an expensive budget (as compared to more traditional organizational functions). However, as described previously, as an organization’s procedures and recruiting/training evolve and that expense will reduce with process efficiencies. CI is usually an Information Technology (IT) component function but often has “dotted-line” reporting and accountability to risk management functions such as internal auditing or the Office of General Counsel. In Law Enforcement, the CI is typically organized into two very different elements: one where computers are used to facilitate crimes (homicide, missing persons, etc.) and one where computers are the object of the crime (network intrusion, malware, etc.). Whether in public or private industry, however, the common practice for CI budget strategy development as a security investigations activity is 10-15% of the IT budget.

The added cost of 10-15% of the IT budget may be "charged-back / "a cost of business impact" to other organizational functions in circumstances such as those involving malicious insiders or users belonging to those functions violating IT or security/risk management policies. As an example of "charge-back", random phishing in which a finance user clicks on a malicious link that causes a Trojan Backdoor installation that is subsequently used to steal funds from corporate accounts could be charged against the finance unit that user belongs to; although, some organizations may choose to generalize information security support costs to IT. Even in the latter case, however, the investigation and remediation could be charged-back to the finance unit.

"Cost of business impact" also occurs if litigation results from the investigative efforts. As a general statement, when dealing with the judiciary, victims of network intrusions must be able to articulate a total financial loss. This can be composed of investigative time spent, recovery/mitigation time spent, and business losses due to network unavailability.

A model for budget strategy development (as a percentage of IT budget) that associates to the previous section as a management framework activity is depicted in the following model.

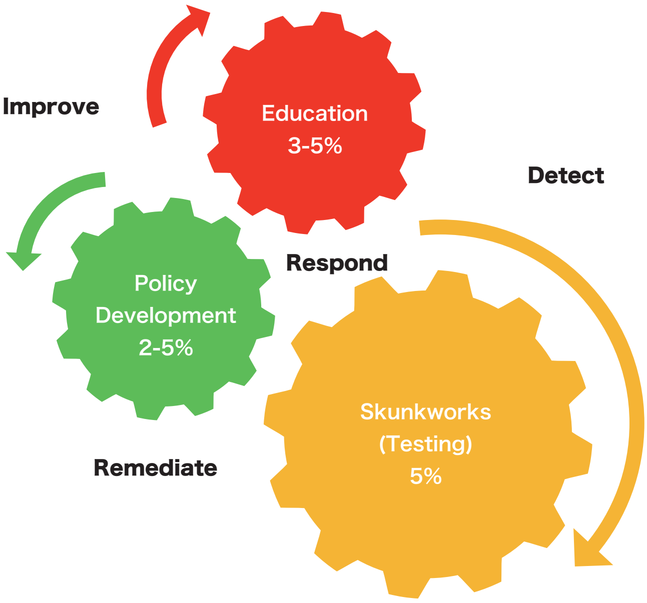


Figure 10-6. CI budget planning strategy

As more specific targeting has evolved against strategic business functions (to interrupt business continuity, steal valuable intellectual property, extort executives or market position, etc.), **corresponding budget allocations in each business function** should similarly be set aside for operating expenses related to cyber investigations and remediation[295]. The more successful a business function is as compared to market competition, the more likely it will be targeted by malicious outsiders or insiders.

[295] Varied allocation models have been presented in industry research, such as represented by SAS – a veteran software company utilized by most global high-finance and operations corporations as well as governments. http://www.sas.com/en_us/insights/articles/risk-fraud/a-modern-cybersecurity-strategy-building-a-budget.html The suggested 10-15% as described is similar to such suggestions but incorporates a charge-back condition for CI budget strategy.

Risk Assessment

Many models have already been defined and adopted in organizations concerning the assessment of information security and related human resources risks. The prevailing standard is International Standards Organization (ISO) 27001 – entitled "Cyber Security Risk Assessment"[296]. The ISO 27001 standard addresses ten risk areas with examination criteria including:

1. Board-led information risk management regime
2. Secure home and mobile working
3. User education and awareness
4. User privilege management
5. Removable media controls
6. Activity monitoring
7. Secure configurations
8. Malware protection
9. Network security
10. Incident management

Crucially, ISO 27001 currently does not include an examination of a CI function, its requisite capabilities, or its related activities. The "Incident management" criteria only address tactical activities and organizational capabilities to identify and respond to an incident, not the collective goals previously outlined as CI strategy. Other standards including NIST-800-series[297], PCI[298], BSI[299], and OCIE[300] also address cyber risk assessments only as an IT security concept, without distinct reconciliation to criminal (or competitive business) objectives that the cybercrime activities seek to achieve. Accordingly, the ISO 31000 "Risk Management" guidance is more appropriately applied, though it converges with issues addressed in ISO 27001, ISO 20000[301] (also related to ITIL[302]), and ISO 22301[303] "Business Continuity".

The closest existing standard to support the CI function is NIST 800-86[304]. However, it currently describes only the process of forensic techniques and procedures for cyber investigations that include collection, examination, analysis, and reporting of related computers or devices. That is only a component activity of the *Respond* goal of the CI function as described.

More development needs to be performed by international cooperative organizations to define and adopt a risk assessment standard for the CI function. The recommended course of action should be to utilize excerpts of ISO 20000/22301/27001 under the framework of ISO 31000 – but focused on the previously described CI goals of "*Detect, Respond, Remediate, and Improve*". Corresponding risk assessment of the CI function should also be included in keeping with ITIL/ITSM (IT Service

[296] http://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security.aspx
[297] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[298] https://www.pcisecuritystandards.org/
[299] http://www.bsigroup.com/en-GB/Cyber-Security/
[300] https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
[301] http://www.itgovernance.co.uk/iso20000.aspx
[302] http://www.itgovernance.co.uk/itil.aspx
[303] http://www.itgovernance.co.uk/bc_dr.aspx
[304] http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Management) guidance such as "Control Objectives for Information and Related Technologies" (COBIT)[305]. A sample taxonomy for CI risk assessment is included in Appendix A.

Risk Management

As with risk assessment, no established risk management standard currently exists for the CI function. COBIT (5) provides a suggested framework for risk management of Enterprise IT that can be adopted for the CI function and integrated into a suitable ITSM framework. The COBIT framework defines seven risk principles for management:

- Connect to enterprise objectives
- Align with Enterprise Risk Management
- Balance cost/benefit of IT risk
- Promote fair and open communication
- Establish "tone at the top" and accountability
- Function as part of daily activities
- Consistent approach

The risk principles are intended to provide a structured approach to risk management that is measurable and can contribute to reliable, objective results that are comparable to similar technical functions of an organization. COBIT uses a set of "Risk Scenarios" to exercise an organization' s capabilities to detect and respond to IT risks in a process depicted in the following figure.

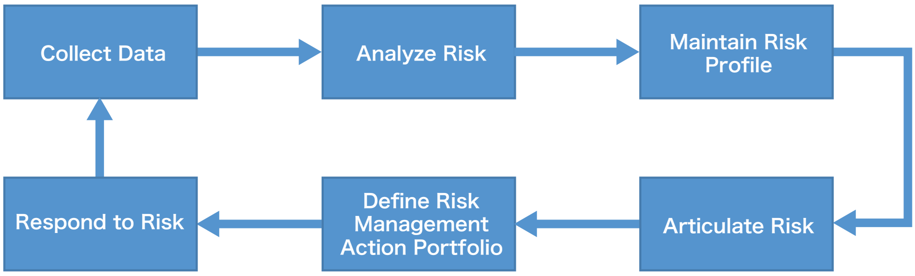


Figure 10-7. COBIT (5) Risk Management Process

The COBIT risk management process has a feedback loop from detection to response regarding IT (and cyber by extension) risks. However, the management process does not include remediation or a process for improvement as previously discussed. The COBIT processes are described in the following figure[306].

[305] http://www.isaca.org/cobit/pages/default.aspx
[306] http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-5-Risk_res_Eng_1213.ppt

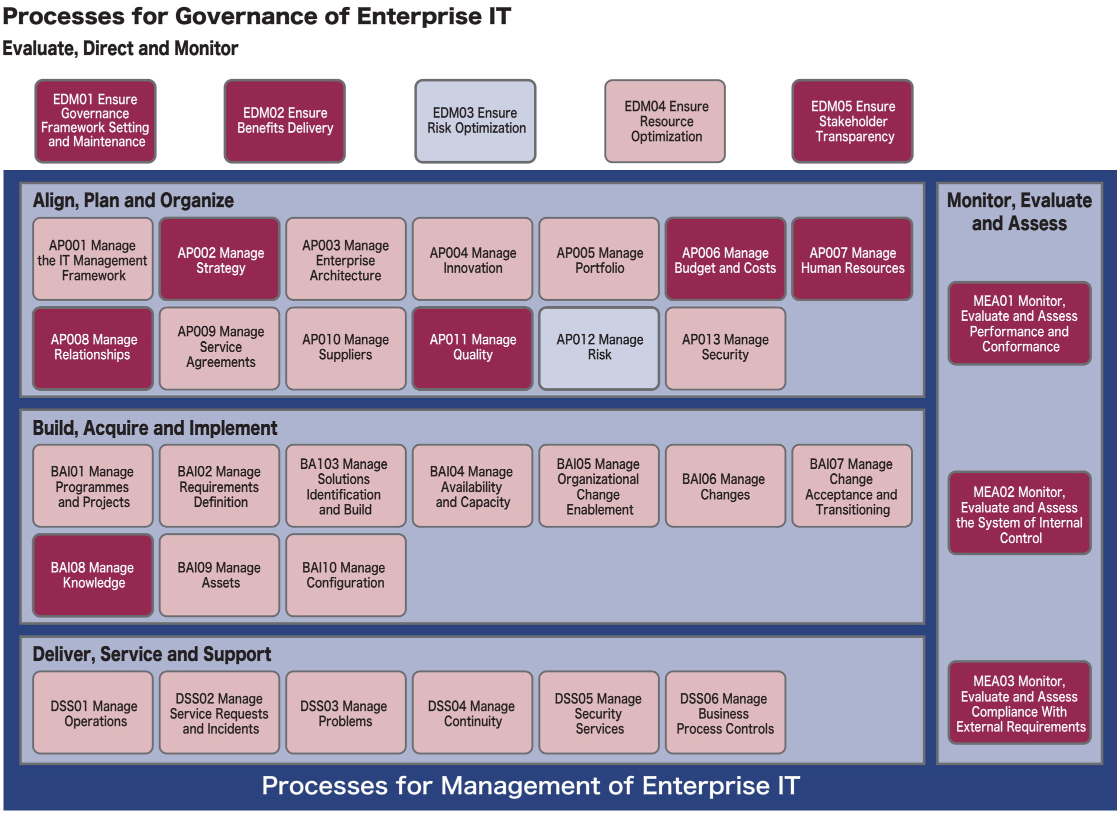

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimization
EDM04 Ensure Resource Optimization
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organize
AP001 Manage the IT Management Framework
AP002 Manage Strategy
AP003 Manage Enterprise Architecture
AP004 Manage Innovation
AP005 Manage Portfolio
AP006 Manage Budget and Costs
AP007 Manage Human Resources
AP008 Manage Relationships
AP009 Manage Service Agreements
AP010 Manage Suppliers
AP011 Manage Quality
AP012 Manage Risk
AP013 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BA103 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organizational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI10 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

Figure 10-8. COBIT (5) Governance Processes

As depicted in the figure, the focus of the COBIT (5) framework is on IT Service Management, not specifically on risk management. Accordingly, although it provides a framework for management, as with ISO 27001 the framework should be adapted to CI function requirements. Depending upon the type of organization, the CI function may be a component activity of IT, or may itself be a functional unit, or may be a support activity of an investigative unit. Thus, no "one-size-fits-all" risk management framework exists. However, the risk scenario focus of the COBIT (5) framework is comparable to CI activities, which focus upon cybercrimes with distinct differentiators in activities to investigate and address cyber risks by type and category.

As noted previously, the rapid development and business penetration of technology, and associated impacts and risks, has in recent years caused an imbalance between the CIO's/CISO's executive authority and responsibility (which will be discussed in detail later in this chapter) versus the potential business impact and loss if the role is performed inadequately. In response to this trend, a movement has been proposed to segregate the roles and executive responsibilities of governance and management, with an aim for healthier corporate management through more effective role-sharing. The COBIT2019[307] framework is an update to COBIT (5) and practically explains this concept and defines the roles and responsibilities of governance and management functions, respectively:

●Governance

- Evaluate stakeholder needs, situations, choices, and focuses; ensure goals are agreed upon based on the defined vision and strategy of the organization
- With prioritization and decision-making, Projects and initiatives most consistent with the

[307] https://www.isaca.org/resources/cobit

organization's goals and strategies are given the highest priority and aligned with the organization's resources to optimize usage
- Ensure the organization's performance against goals and compliance adherence are adequately monitored

The Board of Directors, under the leadership of the Chairman of the Board of Directors, is held responsible for overall governance implementation. It should be noted that the main reasons for governance failure are poor management, lack of sponsorship, lack of flexibility for strategic change, and a perfectionist focus on risk identification while ignoring business alignment. These features must be rectified with the active involvement of the leadership team.

●Management

Management is responsible for planning, building, executing, and evaluating activities in addition to developing strategies, budgeting, and managing resources for various activities to realize goals specified by governance. Under the leadership of the chief executive officer (CEO), executive leaders bear the responsibility for management execution.

The COBIT framework is useful to align business risks with IT/security risks and aids in risk management for enterprise IT. However, its application requires an expert skillset and knowledge of the framework. Often, the complexity of its content makes it difficult to apply in practice. Without a balanced implementation, this may generate administrative overhead- such as "management for management's sake”. Unnecessary overhead should be evaluated through governance-related activities. Two useful approaches for prioritizing and implementing the optimal allocation of limited resources in corporate management are:

- Alignment with Business: Align business strategy with cybersecurity activities using a simplified COBIT framework.
- Risk Profiling: Align business risk with cyber risk (based upon the viewpoint of a cybercriminal’s objective) to classify risks and develop effective risk scenarios.

If combined and managed effectively, risks associated with cybersecurity can be aligned systematically and practically to clarify the organization's management targets and priorities. As a result, the organization will have Consistency in cybersecurity activities and cybercrime investigation functions will be enabled, creating confidence and objective results. Detailed and measurable targets can be set by utilizing extensive key performance indicators (KPIs) for activities.

Using a simplified and tailored COBIT framework is recommended to ensure alignment with business objectives when setting governance and management goals, as complying with all of COBIT's recommendations may be too costly or time-intensive. The COBIT framework consists of components which must be individually defined, by content and depth, within each organization. If skilled governance professionals exist in an organization, a full-scale COBIT framework may be adopted. However, in many cases, extracting and utilizing specified COBIT review steps, design factors, and governance system components is helpful in ensuring business alignment while using available resources. Business alignment should be led by the CIO or CISO, and includes the following steps:

●Understanding drivers and needs of stakeholders

Understanding stakeholder drivers and needs can be achieved through interviews with the board of directors and the leadership team to identify concerns, significant risks, and key issues.

●Setting enterprise, governance, and management goals

When setting enterprise goals, in addition to incorporating stakeholder drivers and needs, the following items from COBIT's Design Factors can be incorporated and should include clear objectives, identified gaps, and action items:

- Understanding of business context and enterprise strategy
- Risk profile
- Compliance with industry laws and regulations
- Threat landscape
- IT security organization function roles
- IT and security issues

●Goal alignment

Goal alignment involves mapping activities to be managed with enterprise goals. The components presented by the COBIT governance system should be used to ensure necessary capabilities are present to support and implement activities in an appropriate and reliable manner. This enables the alignment of business and IT efforts. If capabilities are insufficient, the issue should be escalated to the board of directors, CEO, or other leadership to resolve resource allocation, additional investment, and the alignment of priorities. Capabilities can include:

- Processes
- Organizational structure
- Personnel, skill, and competency
- Data
- Principles, policies, and procedures
- Culture, ethics, and behaviors
- Services, infrastructure, and applications

To effectively set management goals, the current status, the ideal state, and existing gaps around activities should first be clarified during the goal alignment process before setting goals. The CIO or CISO should take responsibility for achieving management goals. If possible, progress should be evaluated every three to six months to enable flexibility to adjust goals in response to changes in enterprise strategy, regulations, and the threat landscape.

To set governance goals, an evaluation of management goals must be undertaken to determine whether they are poised to satisfy the following:

- Setup and maintenance of frameworks prescribed by the organization
- Realization of promised benefits
- Mitigation of risks visualized in the risk profiling

- Optimization of resources
- Commitment to stakeholders

The Board of Directors and leadership team responsible for governance, after making this evaluation, can then provide direction to Heads of Business, the CIO, the CISO, and other executive leaders. The Board, in conjunction with periodic audits, must monitor governance goals around quantitative and qualitative metrics to ensure they are performed correctly and promised benefits are realized.

Risk Mitigation

It is imperative to adopt a risk assessment taxonomy for the management of risks, but a context for discerning which risks to mitigate (whether through control or eradication) requires an evaluation formula or criteria that can be understood by decision-makers. Risk mitigation depends upon understanding the concept of controls (and controls failures). Whereas most investigators (often due to organizational policies or pressures) will search for technical root cause, systemic or program failures are more common – such as users reusing passwords across applications or simply not locking their computers when they leave their desks.

From an investigative perspective, this is why root cause analysis is so important. When technical root causes are distinguished from systemic causes, and coupled with documentation of lessons learned, trends start to emerge that allow for an empirical discussion of risk. Every process includes people, processes, and technology resources and related activities. Because of this, systemic risks cannot be dismissed without remediation, or the organization will continue to suffer incidents.

A commonly used risk assessment formula is:

$$\text{Risk} = (\text{Probability x Impact}) / \text{Ability to Mitigate}$$

By refactoring that formula, the ability of the organization to mitigate a risk should be the result of the probability of a risk condition (or scenario) multiplied by its (estimated) impact divided by the risk:

$$\text{Ability to Mitigate} = (\text{Probability x Impact}) / \text{Risk}$$

Sometimes math doesn' t provide the answer, though. As risk is an empirical value determined by the subjective estimates of probability, impact, and ability to mitigate – it isn' t a simple calculation at all[308]. An organization that seeks to utilize a risk mitigation calculus should adopt a scale for risk classification according to categorical risks (such as type and category of cybercrime).

The scale should be simple and common- a 1-3 (high/medium/low) or 1-10 scale. The Australia/New Zealand ISO 31000:2009 standard "Risk Management – Principles and Guidelines[309]" provides 5 steps to managing risks that include:

[308] Note some IT security risk formulae use "Risk = ((Threat x Vulnerability)/Countermeasures) x Impact"; however as noted those values are subjectively determined.

[309] https://www.standards.govt.nz/search-and-buy-standards/standards-information/risk-managment/

1. Establish the context
2. Identify the risks
3. Analyze the risks
4. Evaluate the risks
5. Treat the risks

ISO 31000 has application to technology management, but included in the described criteria are risk calculus examples such as a common diagram[310] included below.

Figure 10-9. Risk rating for mitigation

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
	Likelihood			

When performing a risk assessment, the calculated severity of an identified risk should be evaluated and mitigated according to its likelihood (probability) to impact the organization. As compared to general IT, however, more complex factors are involved in CI risk assessment.

IT asset risk is often assessed through risk “ranking” such as the following diagram[311] :

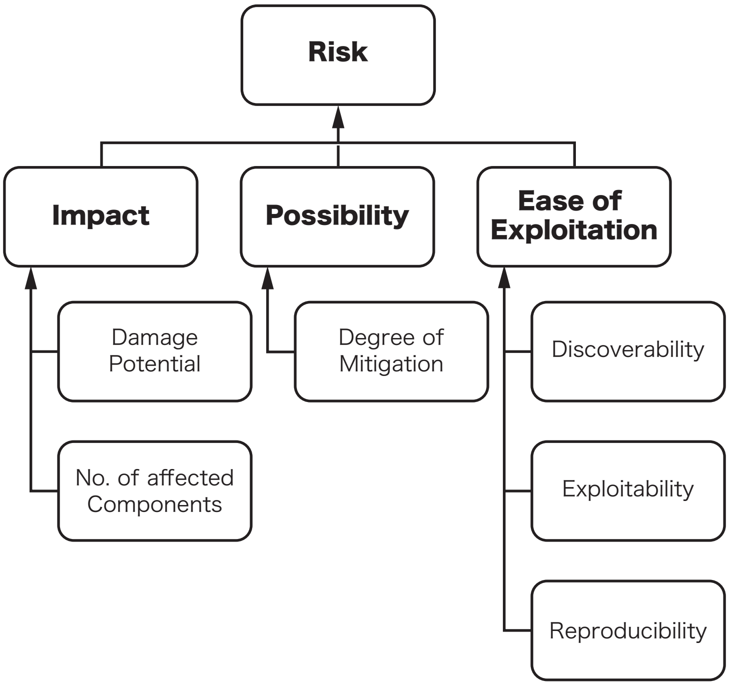


Figure 10-10. OWASP Risk Ranking

[310] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
[311] https://www.owasp.org/index.php/Application_Threat_Modeling

The COBIT (5) scenario approach to risk management can be coupled with the OWASP methodology to define cybercrime scenarios by type and category for the definition of risk mitigation criteria. For example, an organization that has limited user training or awareness of risks related to phishing links will have a higher possibility of cyber risk simply because the ability of the organization to mitigate that risk is limited by user awareness and training. Accordingly, a test scenario to evaluate the risk could be performed by the CI function with a phishing exercise and reporting to executive management, sharing results including the number of users who clicked the link or downloaded an associated backdoor (but did not report such activity).

By performing a simple test of even one of the OWASP criteria, the CI function can describe the potential impact (through research or example) of such an activity – with categorical detail of the possibility of success for that scenario. Such scenarios should reflect historical and current types of attacks or compromises performed by cybercrime actors.

Budget Planning

The budget strategy for planning the CI function was previously described, with different models presented for associating investigations costs to organizational function or support activities – according to the unit association of the CI function. Aside from personnel and tools costs, however, CI typically requires specialized lab facilities and may have associated expenses for certification, etc. Budget planning should therefore include not only personnel costs, but also related expenses.

The *Guide to Computer Forensics and Investigations, 5th Edition*[312] recommends the following:

1. Break costs down into daily, quarterly, and annual expenses
2. Use past investigation expenses to extrapolate expected future costs
3. Expenses for a lab include[313]:
   a. Hardware
   b. Software
   c. Facility space
   d. Trained personnel
4. Estimate the number of computer cases your lab expects to examine
   a. Identify types of computers you' re likely to examine
5. Take into account changes in technology
6. Use statistics to determine what kind of computer crimes are more likely to occur
7. Use this information to plan ahead your lab requirements and costs
8. Check statistics from the Uniform Crime Report[314]
9. Identify crimes committed with specialized software
10. When setting up a lab for a private company, check:
    a. Hardware and software inventory

[312] Nelson, B., Phillips, A., Steuart, C., (2016): Guide to Computer Forensics and Investigations, 5th Edition; Course Technology. Also http://www.utc.edu/center-information-security-assurance/468--ch03.ppt

[313] ASCLAD certification and its peer in Europe are expensive. More and more jurisdictions are requiring this. http://what-when-how.com/forensic-sciences/accreditation-of-forensic-science-laboratories/

[314] http://www.fbi.gov/ucr/ucr.htm

b. Problems reported last year
c. Future developments in computing technology

The Guide also notes that “time management is a major issue when choosing software and hardware to purchase”. As mentioned previously, recruiting and training will help an organization create efficiencies in the CI function. However, training and tools costs are interrelated, meaning both are necessary costs and expense reduction in one depends on a managed increase in the other. Skilled personnel are always a better investment than tools, however, as tools can only be utilized for limited purposes whereas personnel can more readily adapt to case requirements. Hence, always invest in training over tools.

It is also important to consider the labor component of work. Highly-skilled work involves a lot of (relatively) low-level support, a moderate amount of mid-level analysis and development/training, and a smaller (but more important) amount of high-level investigation and reporting. The budget plan should incorporate utility in investigations as factors.

IT budgets in the private sector are typically reflected as a percentage of revenue or as a cost per IT user in the organization. Public sector organizations operate on a cost basis rather than revenue. Exact figures are difficult to estimate for CI functions in the private sector as they are generally “lumped into” IT support costs. Public sector organizations such as Law Enforcement, though, publish their budget requests.

Budget Tracking

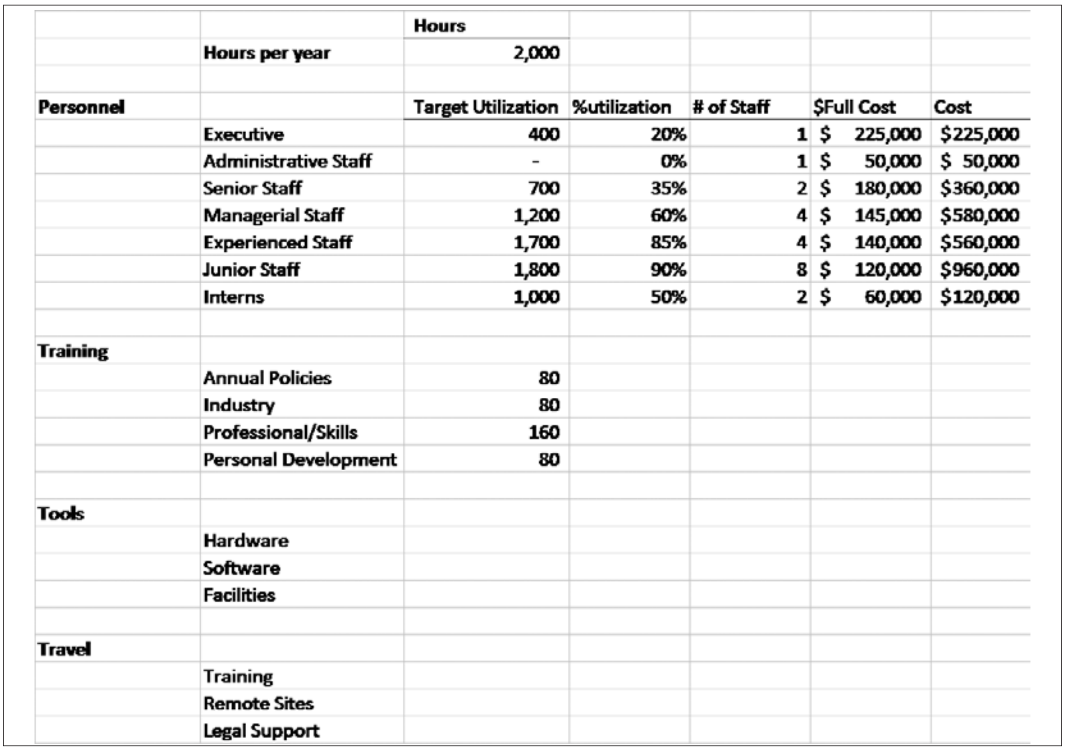
Budget tracking should be performed by a “Time and Expense” system against a budget ledger (single-entry). Direct debits of costs associated with facilities, tools, training, travel, associated expenses, and per-hour (or man-day) time for personnel assigned to the CI function should be accounted for. Charge-backs of time and expenses to other organizational functions, if available, should be credited to the ledger in similar fashion.

Time and expense reporting by personnel should be performed at least weekly, but daily where possible. Associated “Enterprise Resource Planning” software should be utilized for budget planning and tracking/performance purposes – as a shared service of the overall organization. Management expenses (facilities, equipment, and related costs as well as credits by charge-back activities) should be performed as a “Profit and Loss” activity with weekly reporting to executive management, monthly review, and quarterly performance publishing for organizational cost controls. Semi-annual and annual budget reviews should be performed to accommodate emergent budget risks or to report efficiencies to reduce future requirements.

As many CI functions relate to legal investigations, it is recommended that at least hourly time reporting be performed by staff. In some cases it may even be necessary to report quarter-hours and breakdown expenses by different categories for tax purposes.

Resource Utilization Tracking

Resource utilization (tools, equipment, and personnel) should be correlated to time and expense tracking policies and related procedures. The general figure used for technical personnel tracking purposes in the U.S. is 2,000 hours per man-year of “billable” time or expected utilization. A matrix of resource utility related to that figure should be incorporated to ensure high quality of job satisfaction, however, or the organization will face corresponding turnover. Performance should be measured in the budget matrix.



		Hours				
	Hours per year	2,000				
Personnel		Target Utilization	%utilization	# of Staff	$Full Cost	Cost
	Executive	400	20%	1	$ 225,000	$225,000
	Administrative Staff	-	0%	1	$ 50,000	$ 50,000
	Senior Staff	700	35%	2	$ 180,000	$360,000
	Managerial Staff	1,200	60%	4	$ 145,000	$580,000
	Experienced Staff	1,700	85%	4	$ 140,000	$560,000
	Junior Staff	1,800	90%	8	$ 120,000	$960,000
	Interns	1,000	50%	2	$ 60,000	$120,000
Training						
	Annual Policies	80				
	Industry	80				
	Professional/Skills	160				
	Personal Development	80				
Tools						
	Hardware					
	Software					
	Facilities					
Travel						
	Training					
	Remote Sites					
	Legal Support					

Figure 10-11. Simple budget tracking example

Budget Process Improvement

As time and expenses are tracked to the budget plan, performance should be compared to the budget strategy as planned and agreed with organizational leadership. Opportunities to charge-back related resource allocations to supported organizational functions should also be reviewed in order to adjust cost management or resource requirements. Monthly and quarterly performance reviews should be performed by functional area executives, and biannual and annual performance should be reported to organizational leadership for strategic planning support.

Human Resources

Human resources are the heart of any organization. No matter how many tools, processes, procedures, or rules are defined and implemented, unless there are people who are willing to lead and people who are willing to follow their leadership, there will be no organization. Highly technical fields of work such as cyber investigations are challenging to recruit, hire, and retain for related jobs. The market for their skills and talents (and more importantly their *experience*) is among the very most competitive. Careful consideration of the scarcity of those resources- and the critical nature of their work with regard to helping an organization successfully defend against, or investigate incidents of, cybercrimes – should be made.

Defining Human Resources Organization

The human resources required for the CI function include executive, administrative, senior (Expert), managerial, experienced (Journeyman), and junior staff. As cyber investigations involve evolving technologies, it is also highly recommended that interns be included as a (limited engagement) staff position. Interns serve as a fresh source of knowledge and as a recruiting pool for potential talent to advance the capabilities of the CI function and staff. A hierarchical structure based upon knowledge and skills is suggested, but with collateral engagement of senior and experienced staff with junior staff in a matrix task-oriented resource utilization. This ensures skill and experience development (similar to assigning junior investigators to senior investigators in police and federal law enforcement activities). Executive and managerial staff should be domain-experienced but interleaved based upon experience in the CI function according to related talent requirements (investigations, intelligence, forensics, and related judiciary and public relations support activities).

As explained in this book' s introduction, cybersecurity is an IT function designed to identify and mitigate organizational risks. Cybersecurity can be thought of as "cybersecurity risk management". Although its precise nature varies across organizations, it is fundamentally an area of enterprise risk management with the purpose of defending management and business strategies and the business itself against cyber risks. As a management function, it is responsible for mitigating risks to the entire business and fulfills executive management (EMS) responsibilities to customers, markets, shareholders, and investors.

To properly execute these tasks, organizations have increasingly established the positions of Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) as strategic management roles. In addition, the core members of the cybersecurity function have expanded to include the Board of Directors and C-Suite for governance, and executive leadership including Chief Business Officers (CBOs) for management.

As a result of the rapid development of technology and its penetration into business, the number and the magnitude of impact of cyber incidents have expanded. At the same time, CIO and CISO executive authority and responsibilities have not been balanced with business impact and loss, resulting in unbalanced risk management for many enterprises. To be proactive in risk management, enterprises must understand cyber risks from a business-wide impact perspective, review roles and responsibilities including those of executive leadership, clarify governance responsibilities such as those of the board of directors, and transition to a leadership-friendly management structure.

CISOs oversee a wide variety of security activities, bear responsibility for setting goals for various security functions, and develop organizational and human resource strategies and budgets to achieve those goals. Therefore, CISOs are required to be more than simply a security expert- they must have a thorough understanding of the business domain, including management and business strategies. If CISOs take actions that only pursue security objectives, security teams will eventually be at odds with business teams. Therefore, CISOs must develop security strategies that align with management and business strategies. EC-Council University cites the following as “6 Keys for a Successful CISO”[315]:

1. CISOs Align Plans with Core Objectives

[315] EC Council University Blog- 6 KEY CHARACTERISTICS OF A SUCCESSFUL CISO. https://blog.eccu.edu/6-key-characteristics-of-a-successful-ciso/

2. CISOs Require Leadership Skills for Successful Execution
3. CISOs are Responsible for Interdepartmental Coordination and Delegation
4. Continuous Learning is the Key Feature of a CISO
5. CISO is a C-Level Executive
6. CISOs Create Benchmarks

Once a cyber incident occurs, it is rare for an organization to be able to complete an incident investigation with internal resources alone. Many organizations are forced to work with outside experts. However, many lack the preparation and understanding of protocols to work with outside experts, preventing collaborations from occurring quickly and smoothly and impairing the evidence necessary to investigate cybercrimes. Fortunately, successful collaboration between police, law enforcement, and enterprises in physical security responses has frequently occurred and provides a glimpse into the potential benefits of doing so, which include:

- Education and guidance to prevent those in vulnerable positions from being victimized.
- Effective precautions and measures
- Early response to incidents to minimize damage
- Strengthening the organization's ability to protect its reputation
- Deterring criminals through proper preservation of evidence, investigations, and arrests

It is imperative that in addition to facilitating an effective internal CI function, organizations take steps to ensure beneficial collaborations with external parties who work alongside internal staff during investigations.

Defining Jobs

According to whether the CI function supports a public or private sector organization, jobs will differ primarily with regard to judiciary and public relations roles. Investigations, intelligence, forensics, and administration jobs are otherwise common to both sectors. Jobs should be defined according to the resource requirements that the organization is tasked to address, as determined by the types and categories of cybercrimes that the organization has faced in the past and is projected to face in the future.

Traditionally, security governance and management have not been segregated, and centralized structures with dedicated security teams responsible for all security measures and responsibilities have been common. Today, as cyber threats increasingly impact businesses, the authority and accountability delegated to security teams is often disproportionate to the scale and severity of business impacts. Therefore, a management structure based on the Three-Line Model[316] of the COSO (Committee of Sponsoring Organizations of the Treadway Commission)[317] may be helpful in facilitating a more effective division of responsibilities and roles within organizations:

[316] THE IIA'S THREE LINES MODEL ~ An update of the Three Lines of Defense, 2020, The Institute of Internal Auditors, Inc.

[317] COSO (Committee of Sponsoring Organizations of the Treadway Commission) Treadway Committee Organizing Committee https://www.coso.org/

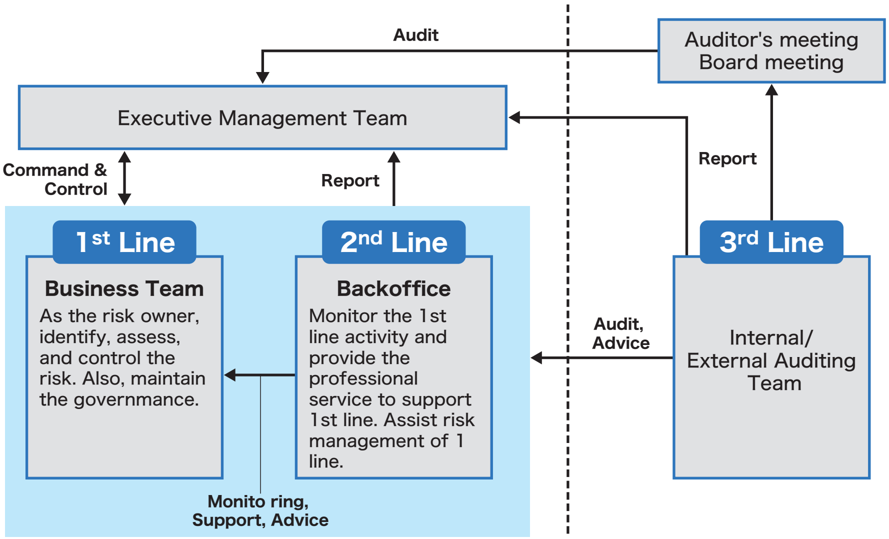

Audit
Auditor's meeting
Board meeting
Executive Management Team
Report
Command &
Control
Report
1st Line
2nd Line
3rd Line
Business Team
As the risk owner, identify, assess, and control the risk. Also, maintain the governance.
Backoffice
Monitor the 1st line activity and provide the professional service to support 1st line. Assist risk management of 1 line.
Audit,
Advice
Internal/
External Auditing
Team
Monito ring,
Support, Advice

Figure 10-12. Three-line Model

●1st Line: Business Department

The 1st line can most accurately recognize the nature of the business, its execution, profits and losses, and potential impacts from risks to the business. As the owner of risks associated with the business, it must bear the responsibility to assess, identify, control, and uphold governance of risks. Since the 1st line rarely has significant security or risk management expertise, it must be supported by the 2nd line.

●2nd Line: Indirect Administration Department

The 2nd line is comprised of security related functions requiring a high level of expertise including security management measures (policy and rule development, solution implementation and operation), security monitoring (SOC), incident response, information gathering and sharing, IT infrastructure management, asset management, risk assessment, account management, access rights management, application management, vulnerability response, disaster recovery, security education, enlightenment, and training. All of these functions require the involvement of the entire organization, but the 2nd line takes the lead in performing these tasks.

Critically, the 2nd line must align these tasks with the 1st line' s risk perceptions and priorities to avoid disagreements over business targets and values to be protected. Without alignment, the 2nd line can become perceived as an internal adversary slowing down business progress. Antagonistic structures and discourse can become a source of vulnerability for an organization, and as such, the 2nd line must be sensitive to business needs to avoid undue risk.

●3rd Line: Internal Audit Department

The 3rd line must objectively evaluate the 1st and 2nd line security efforts within the organization and maintain the organization's independence, primarily through security and compliance audits.

In addition, outsourcing to external providers with expertise may be required if in-house resources and capacity are insufficient. Functions requiring advanced security skills such as security monitoring (SOC) and incident investigation (forensic investigation) can be outsourced to trusted external specialists.

To strategically link outsourcing partners with organizational goals, it is critical to share information and KPIs associated with governance and management goals. When activities of external outsourcing partners are uncoordinated, limited resources are consumed, causing business-critical risks and attack vectors to be overlooked. Applying business-aligned priorities across supply chain partners engaged in cybersecurity activities enables robust implementation of and control over security monitoring and incident response.

The figure below integrates outsourcing partners to the NIST CSF's five core functional categories (IPDRR) of necessary security functions, in alignment with the three-line model. Security activities and functions should be managed according to each organization' s context, to help clarify roles and responsibilities.

Figure 10-13. Examples of Necessary Functions for Security Activities

	Identify	Protect	Detect	Respond	Recover
1st Line	Asset, account (ID), device, application management/ Risk Assessment	Vulnerability response, security policy governance	Crisis management, Business Continuity Management		
	Supply chain management, Risk management, Product/service security, Training, awareness				
2nd Line	Asset, account (ID), device, application management (for common)	Security control(s), Monitoring, Vulnerability response (for common)	Incident response, Disaster Recovery, Information Sharing		
	Learn and improve Evaluate performance for improvement				
3rd Line	Security Audit				
External	Security Audit	Provide solution		Incident response	

Human Resource Utilization Planning

As depicted in the previous budget tracking example, different levels of utilization in the organization of human resources should be planned. Although reduced utilization of resources occurs with more seniority in job roles (partly due to administrative or other organizational activities, such as public relations in Law Enforcement or strategic planning in private sector companies), greater efficiencies in the performance of work are produced. Highly technical jobs have limited talent pools available to draw from, both internally as well as externally. Accordingly, an organization should understand the effective human resource utilization of job roles.

Human Resource Performance Management

Human resource performance in highly-skilled jobs should be a measure of adherence to policies, subjective association of confidence in leadership abilities (whether technical, task management, or personnel - or a combination of all), and objective attainment of resource utilization planning objectives. As the CI function budget requires daily (or at least weekly) time and expense reporting, weekly and monthly performance to utilization targets should be provided. Subjective performance assessments of leadership as well as objective policy adherence (or violations and related impact) should be performed quarterly and annually as well. Annual performance should be associated with pay and benefits reviews in order to correlate with organizational strategic planning requirements.

Defining Skillsets

The major jobs in the CI function involve investigations (human and technical), intelligence (reconnaissance, monitoring, and source development), forensics (computer/mobile device and network), and administrative or support (such as public relations or judiciary). The primary CI activities of investigations, intelligence, and forensics require a common technical foundation – and specific experience and developed knowledge to perform at senior levels, or to expert requirements[318].

At a minimum, a working knowledge of major computer operating systems and inter-networking protocols and how to operate related investigative or assessment tools (for testing, collecting evidence, or performing forensics and data analysis) are requirements of those performing primary CI activities.

Administrative, managerial, and executive staff roles also require business functional education and training. Other support functions including judiciary and public relations are highly specialized skills supported by focused academics and industry-specific training and exposure.

Skillsets for primary CI activities should be defined according to knowledge and experience requirements that align with roles for human resources planning and utilization. The following model provided by Project GLACY depicts such requirements according to job roles by type and category of cybercrimes that CI activities relate to.

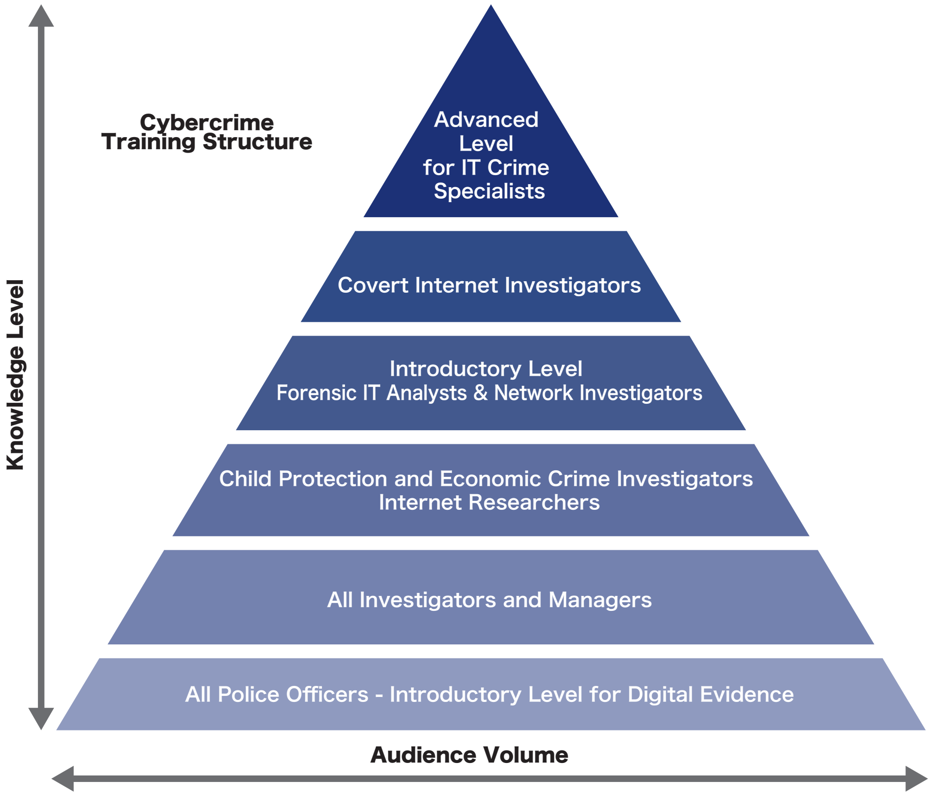

Cybercrime Training Structure
Knowledge Level
Advanced Level for IT Crime Specialists
Covert Internet Investigators
Introductory Level Forensic IT Analysts & Network Investigators
Child Protection and Economic Crime Investigators Internet Researchers
All Investigators and Managers
All Police Officers - Introductory Level for Digital Evidence
Audience Volume

Figure 10-14. Project GLACY skills association to the CI function

[318] "Expert" requirements in CI may involve reporting or testimony (in deposition or court).

Recruiting and Hiring

As previously discussed, a developed CI function should incorporate interns into its human resources planning as a means of identifying potential talent (and providing fresh knowledge of evolving technologies). All highly-technical and specialized fields of work suffer high turnover in employees. Because of this, constant recruiting and hiring should be a planned activity, and a performance objective for managerial and executive staff.

Recruiting from colleges and universities will provide adaptive and eager minds seeking experience that can benefit an organization. However, hiring from trade schools and military or experienced (and "trained-to-task") talent will provide needed field experience and hard skills that only real-world exposure can bring. Federal/regional/local law enforcement, military, or similar experience from associated CI functions serve as excellent education and experience sources for certain functions. Both are necessary talent pools to focus recruiting and hiring upon, across public and private sector organizations. The following matrix provides a simple calculus for recruiting around CI activities:

Figure 10-15. Recruiting CI Targets by Activities

Role	Education	Experience
Executive	University	High (any CI activities) — Public and Private
Investigations	University or Federal	High-Medium Public or Private
Intelligence	University and Federal	High Public (preferred)
Forensics	University or Trade School or Industry	Medium Public or Private
Administrative	University or Trade School or Industry	Medium-Low Public or Private
Judiciary	University and Industry	High Public or Private (preferred)
Public Relations	Industry or Federal	High Public (preferred)
Support	Industry or Federal	Medium Public or Private

Skills Performance Objectives

Skills performance objectives should be calculated for measurements of required activities personnel perform, as well as associated training outcomes from recurring training (delivery in the case of senior staff, or accomplishment by other staff). This should also be factored by experience levels staff currently occupy in their job role, as well as projected achievements in annual performance reviews if they are seeking advancement.

Skills and Knowledge Verification

As a highly-technical field, particularly at senior levels, skills and knowledge verification should be performed during recruiting, hiring, and after a performance "testing" period of employment to ensure adequate staffing according to the CI activities personnel will perform in the organization. Verification of technical capabilities should be performed by senior staff in mentored work sessions where possible, and leadership aptitude or capabilities should be assessed through objective surveys by executive/managerial and junior staff. Judiciary, administrative, and support staff skills and knowledge should be verified by personnel in comparable activities in the organization, though final determination of suitability to the role should revert to the executive staff of the CI function through the hiring manager.

Performance Management

Performance management is an important strategic reporting activity of any organizational function. In order to grow or develop the CI function, leadership must be able to articulate measurable performance to established standards and plans (that they should participate in creating).

Organizational Performance Metrics

Measuring the CI function for success or identifying weaknesses in performance is difficult as cybercrimes are targeted at individuals or organizations, not activities that form the "normal course of business" (although they have become a somewhat normal course for organizations to respond to). Tactical and strategic risks that the CI function should relate to were discussed previously in planning and management sections. Organizational performance metrics should be applied according to risk management or other organizational performance criteria, as a function of the organization or unit that the CI function is assigned to support.

Organizational Auditing

Auditing the CI function should be performed according to resource(s) planning, allocation, and performance to plans on a monthly, quarterly, and at least annual basis in order to inform the organization for strategic budgeting and planning activities. Auditing should be implemented according to test plans concerning governing procedures that include processes that the CI function is responsible for performing.

Operational Process Metrics

Operational process metrics of the CI function should generally be determined according to the same criteria of overall organizational metrics. For example, finance and IT are generally technical fields with similar skills and knowledge intensities as CI activities. Both are support functions of an organization and have defined (and auditable) risk management processes. The previously mentioned COBIT framework provides a means for measuring risk and corresponding performance to operational objectives. In public sector CI function activities (Law Enforcement investigators, etc.), the operational process metrics should be more similar to coincidental public sector roles (such as forensic pathologists vs. computer scientists, or HUMINT vs. ELINT intelligence specialists, etc.).

Operational Process Auditing

Any job can be measured for performance. Any work performed should have associated processes and procedures, as well as activity reporting (time, expense, resource utilization, etc.). As such, any job can be audited for adherence to procedures and operational guidance. The activities performed by CI staff will define specific operational processes such as investigative and intelligence procedures that include evidence collection and processing, as well as judiciary or public relations reporting and communications. Procedures should be well-defined to the CI activities performed by staff and operational processes should be performed regularly to ensure adherence to policies – as well as to identify requirements for or opportunities to improve related procedures. Audits should be transparent and open to review.

Performance Measurement and Improvement

By regularly auditing operational processes and procedures, staff performance will be standardized and efficiencies of scale (of resources allocation and utilization) should be gained. If no gains are achieved, then additional audits should be performed on both personnel and related operational processes in order to determine weaknesses in human resources or operations that can be corrected. By auditing, both staff and organizational performance can be improved.

People Management

Management of people is much more than a "resource management" activity. People have motivations and desires. Highly-skilled technical experts have motivations to succeed, to be recognized and rewarded, to challenge their peers and staff intellectually, and to seek education opportunities. Managing people in technical organizations or functions means gaining trust, demonstrating knowledge (including admitting what you "don' t know"), and providing leadership by example.

Group Dynamics

As previously mentioned, the CI function is a highly-technical field of work and human resources planning and organization requires an interleaving of talents, experience, and management for efficient organizational performance. The pairing of senior and junior task-oriented staff ensures collaboration through a mentoring approach to skills and experience development. The interleaving of managerial and executive staff with junior and senior staff provides opportunities (and options) for the advancement of personal and professional development objectives. These designs in organizational human resources planning are intended to create homogenous group dynamics to foster open dialogue, technical consistency of work performance, longevity of service, and engagement of staff to organizational strategic objectives.

Building Learning Organizations

A learning organization is one composed of strong group dynamics and open communication, while also measuring performance to identify strengths, weaknesses, and opportunities to improve. The CI function, if constructed as previously described with interleaved roles, will incorporate learning into the structure of the organization. This will enable continuous improvement.

Coaching

Managerial staff, coaching for junior staff, and support activities for highly technical risk management activities are important. No organization that appreciates potential or has experienced actual impacts of cybercrimes can afford turnover in staff that must necessarily understand the intricacies of not only the business but also the personnel and architecture of the organization. Coaching should therefore be not only a function of CI activities, but also a collaborative effort of the organization where CI supports other strategic goals.

For example, CI investigators specializing in financial crimes should be coached not only by forensic computer investigators, but also accountants or controllers in order to help develop the investigator' s understanding and appreciation of the domain-specific risks that will inform their comprehension as they analyze collected evidence. As those investigators become more experienced in financial investigations, their efficiency of work will increase, business interruption of their activities will decrease (improving related organizational performance), and their value to the organization will consequently increase – including in their value to develop other staff skills and knowledge. If those investigators are not coached properly by both the CI function as well as the business function they support (Finance), they may leave the organization and the time and expense in their development leave with them.

Team Building

Leadership requires followers. Followers cannot simply be assigned; they must be willing to be led. That is made possible by demonstrated knowledge, skills, and experience that followers appreciate in a leader. A true leader is sought out by junior staff (or others) for opportunities to develop their own skills and knowledge. Just like a client doesn' t become a "customer" until the second purchase of a product or service, a leader is made the second time staff chooses to follow them.

Team building in CI activities should be a function of human resources planning around functional requirements to support the organization and assist in managing related risks. Team building must also be a function of human resources performance management to ensure that followers are provided with leaders they can appreciate. If not, turnover will occur and operational performance will suffer.

Motivation Management

Every individual has personal and professional motives for success. Whether basic motives of health and safety or advanced motives of self-actualization[319], they are individual motives. A well-managed organization will plan for the satisfaction of personal needs within the context of operational performance requirements. This is achieved partly through the matching of functional skills and knowledge to budget planning for recruiting, hiring, employing personnel at tolerable levels of utilization. It is also achieved through proper organizational planning for roles and associated coaching and mentoring.

Highly-skilled personnel are in high demand in industry,and are often highly sensitive to criticism or negative feedback. A well-managed organization will create an atmosphere of leadership and management policies that improve performance without derogatory feedback.

Multi-cultural Environment Management

Complex tasks require complex minds and broad experiences gained from broad exposures to environments and cultures. Cybercrimes are not committed only in one geography, nor are they committed only by one ethnicity or demographic. Perhaps more than any other job, the CI function demands a multi-cultural environment and open-minded/progressive staff. Due to the origins of cybercrimes and the victims of such activities, it is often necessary for CI staff to travel to support related investigations. Similar open-minded and integrated cultural experiences can help a CI function to improve its performance.

[319] See Maslow's hierarchy of needs: http://www.simplypsychology.org/maslow.html

Tool Management

Selecting the right tools for the job is an important planning activity. Tools can facilitate efficiency in work and reduce time and expenses from third-party contract support for incidental costs associated with cybercrime investigations.

Tool Selection for Strategic Needs

Strategic objectives of a business define infrastructure requirements, which in turn generally define the support (policies, procedures, technology, and personnel) needed to help the organization achieve those objectives. Strategic organizational capabilities to communicate securely, document and manage information in the conduct of their activities, securely manage non-public and private data, and protect competitive secrets have corresponding CI requirements.

At a minimum, an organization should invest in the following tools to support strategic needs:

1. Perimeter network and communications (email and voice) monitoring tools
2. Antivirus and anti-malware software and hardware
3. Security Information and Event Management (SIEM) software
4. Forensic computer, mobile device, memory, and network acquisition tools
5. Data retention and analytics tools

Tool Selection for Tactical Needs

Whereas strategic tools will be utilized each day to support the organization, more sporadic tactical needs will arise that should be planned for as well. At a minimum, an organization should invest in the following tactical tools to support organizational needs:

1. Rapid deployment forensic kits
2. Memory analytics software
3. (Network and host) scanning and assessment software and hardware
4. Open Source and Proprietary Intelligence software or services
5. Recording (audio and video) equipment or services
6. “Sandbox” software and hardware or services
7. “Sinkhole” software or services
8. Reverse engineering and analysis software
9. “Stingers” or antivirus/malware discovery software
10. Two-way radios or “clean” cell phones and mobile devices (iPad, etc.)

Tool Use Tracking and Performance Review

The value of tools can only be measured by their utilization as an asset. Tools that are never taken off the shelf are a cost to the organization without a corresponding value. Tools that are never available because they are important to the performance of a task but under provisioned are an opportunity cost to the organization affecting its efficiency and productivity. Tools that support strategic needs of the business are IT investments that should be tracked according to related budget planning, However, tactical tool usage should be tracked through utilization metrics by personnel in their time and expense reporting. At least quarterly, utility and performance reviews should be conducted by CI staff to determine whether related tools are sufficient or could be improved or discarded from the CI inventory.

Tool Training and Certification

Staff training on tools selected to support the strategic and tactical needs of the organization (or the supported function) is critical for efficient budget planning and execution of the CI function. Some certifications are available from industry training sources, but roles-based certifications should be defined by the organization according to the CI activities that support strategic functional goals (detect, respond, remediate, and improve). Training objectives to achieve (internal and/or external) certification should be documented and included in performance metrics for human resource planning.

Chapter 10: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

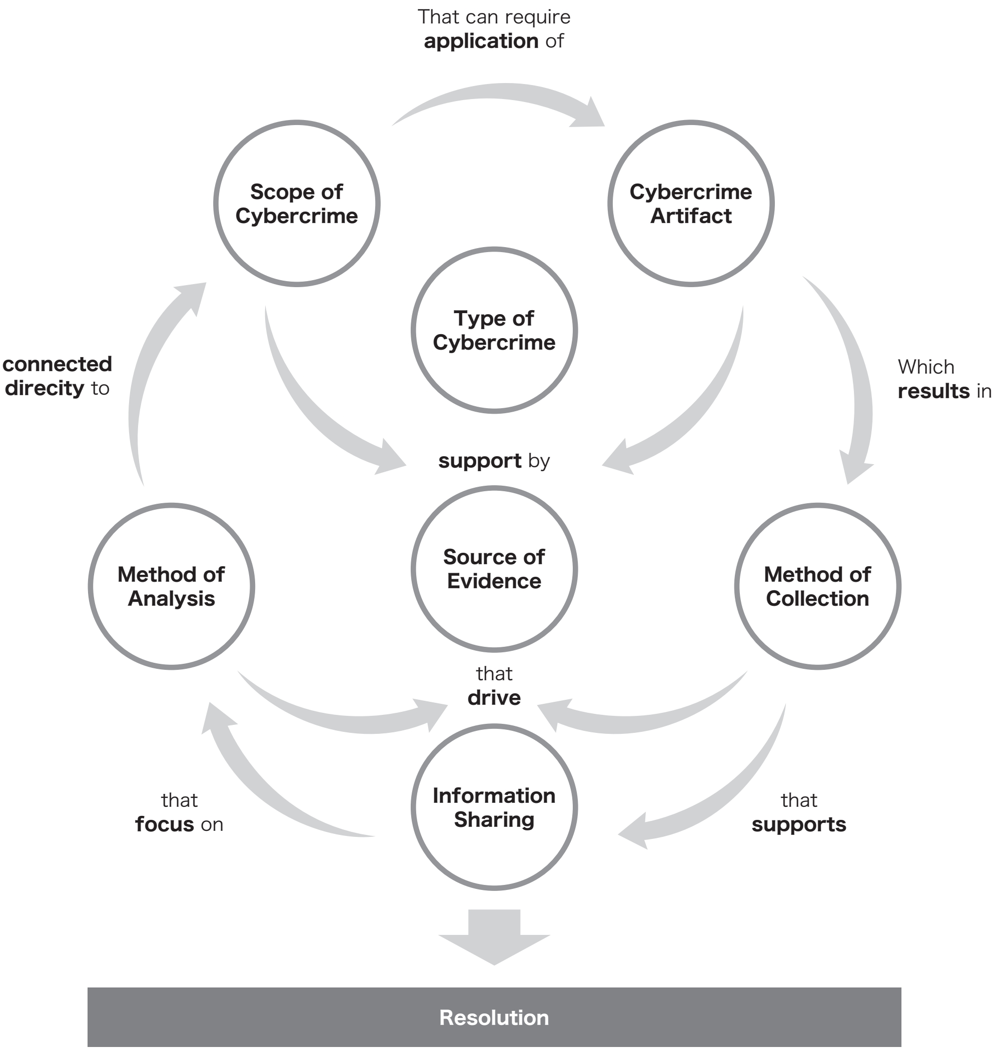


Figure 10-16. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 10-15. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 10-16. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should develop policies, procedures, and plans – and manage the (human and other) resources and their continuing development.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. Intelligence staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigations staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will provide restrictions and penalties for the sharing of information. Senior staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The scope of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when, according to which organization/functions/personnel are affected. Senior staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Support – require procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 10: Review

1. What is the purpose of a cybercrime investigation and resolution function?

   Answer: To investigate alerts or direct responses to legal requests.

   Examples: Breach of PII managing system, misuse of a user account to access financial data, etc.

2. How should the function be organized and managed?

   Answer: Strategically and managed by experienced staff

   Examples: As a supporting function of risk management by experienced investigators

3. What is the strategic objective of the function?

   Answer: Detect, Respond, Remediate, Improve

   Examples: Plan and allocate resources (human, time, finance, and tools/equipment)

4. What are the resource requirements (staff, tools, and community) of the function?

   Answer: Experience, technical/approved or used in standard practice, industry/research

   Examples: Executive, Intelligence, Investigation, Judiciary, Support, Administrative, Hardware/Software/processing systems and facilities

5. What are the technical and experiential requirements to staff, manage, and lead/govern the function?

   Answer: Senior, Mid-level, Staff, Intern

   Examples: education, knowledge, skills and (case/investigations) experience

6. How should the function' s (and related staff' s) performance be measured?

   Answer: By standards to policy and results

   Examples: According to policies and staff development success

7. What organizational communications and strategic involvement, and in which organizational channels, should be implemented for success?

   Answer: Planning, performance metrics

   Examples: (human resources, budget, and tools) in functional and strategic reporting

8. Which organizational executive function(s) should the cybercrime investigations and resolution function report to?

   Answer: Risk management

   Examples: coordination/matrix reporting with CIO, GC, GA as appropriate

Case Study 10: Cyber Security Risk Ownership

- **Crime**: Information theft
- **Suspect(s)**: Access broker
- **Means**: Social engineering using USB sticks
- **Motive**: To test employee security awareness and security architecture
- **Opportunity**: Facilitated by corporate executive

In 2015, the CIO of a global company headquartered in Tokyo hired a cybercrime investigator to assess the firm' s security posture around data loss through social engineering, phishing, or other means. After further discussions, the investigator developed a simple USB drop exercise that would be executed at the corporate headquarters. The purpose of the exercise was to determine the effectiveness of the company' s employee cybersecurity awareness training while coincidentally testing the adequacy of its security architecture (from endpoints through the network).

First, the investigator created a web service registered to a cloud server in Ukraine. An infostealer was then programmed to automatically run from a USB stick when inserted into a Windows computer. The infostealer was built to collect data including the date and time, IP address, hostname, username, operating system, and browser build. Once the USB was inserted into a Windows device, the infostealer would send this information with a unique device identifier to a DNS registered to the aforementioned cloud server. The DNS was from a dynamic DNS provider and the registration was less than 1 month old with a repurposed certificate.

The infostealer malware was copied onto 40 new USB sticks, each of which was labeled with the company logo and an inconsequential serial number. The only files on the USB sticks were the infostealer malware, named "autorun.inf", and a blank Word document. The investigator proceeded to send 10 USB sticks in envelopes printed with the company logo and addressed to random executives at the corporate headquarters (the list of executives was compiled through a rudimentary internet search). The remaining 30 USB sticks were taken to the corporate headquarters where, during a public tour, the investigator placed 20 in a basket in a coffee break room and dropped the remaining 10 randomly in hallways and on desks.

The investigator then monitored the cloud server hosted in the Ukraine and within two weeks, all 40 USB sticks had communicated at least one computer' s information from the corporate headquarters. In some cases, USB sticks had been used with personal computers as well. In total, information from 89 distinct computers and 45 distinct users was conveyed to the web server- from an initial deployment of just 40 USB sticks.

A subsequent review with corporate security revealed no documented help desk calls about the USB sticks, even though employee awareness training highlighted caution against the use of unknown USBs and devices. In addition, the company' s security architecture did not detect any network anomalies, even though communications from the corporate Tokyo office to Ukraine web services were extreme outliers based on normal historical patterns. No DNS or certificate history/warning systems were employed by the company and only 5 antivirus alerts were discovered in the company' s console logs, even though autorun files on USB sticks had been known to represent a significant malware threat for over ten years.

Based on the results of the exercise, the company invested in security policies and supporting tools to raise and monitor employee security awareness, as well as network and endpoint communications and data loss defenses.

Chapter 11

Practical Cyber Risk Management

Introduction

The ultimate objective of the cybercrime investigations unit is to protect mission critical assets and reduce the risk of business disruptions, while aligning its management system with business strategies and corporate risk management (as discussed in Chapter 10). Ideally, organizations should build cyber risk management and IT service management functions into business strategy based on enterprise strategic functions, managed by a holistic framework aligning with enterprise management. However, this requires strong leadership and enormous amounts of resources (and time) given the wide scope of enterprise management. While this is the ideal approach, it may not always be achievable.

This chapter proposes an approach to practically integrate cyber risk management with business strategy requirements.

- Acknowledgement and increased integrity of business risk management.
- A shared definition and understanding of threats (and their origins), vulnerabilities, risks, and impacts.
- Greater integrity of strategy and activities (especially objectives and scope) for the cybercrime investigations unit.
- Greater organizational capability for cyber risk management.
- Specified technical requirements for cyber risk management, both to address legal and procedural needs during investigations (ex: how long to retain logs for investigation)
- Improved incident response and resource distribution based upon risk prioritization.
- Greater discernment of misdirection tactics, such as false flags, in order to identify critical indicators.

In addition, the integration of existing management frameworks (such as COBIT) into the scope of cybercrime investigation activities will be demonstrated.

At the conclusion of this chapter, readers will have understanding of:

- How can risk management frameworks be implemented in practice?
- How should risk management practices be aligned with business requirements and operations?
- How is risk management relevant to cyber threats, vulnerabilities, and risks?
- How should assets requiring protection be identified?
- How should risk scenarios be created and evaluated?
- How should risks be evaluated?
- How should risk response be implemented?
- How and when should risk levels be monitored?
- How and when should risk reporting be presented to executives?

Topic in Practical Cyber Risk Management

The following figure displays topic categories in the “Practical Cyber Risk Management” knowledge domain.

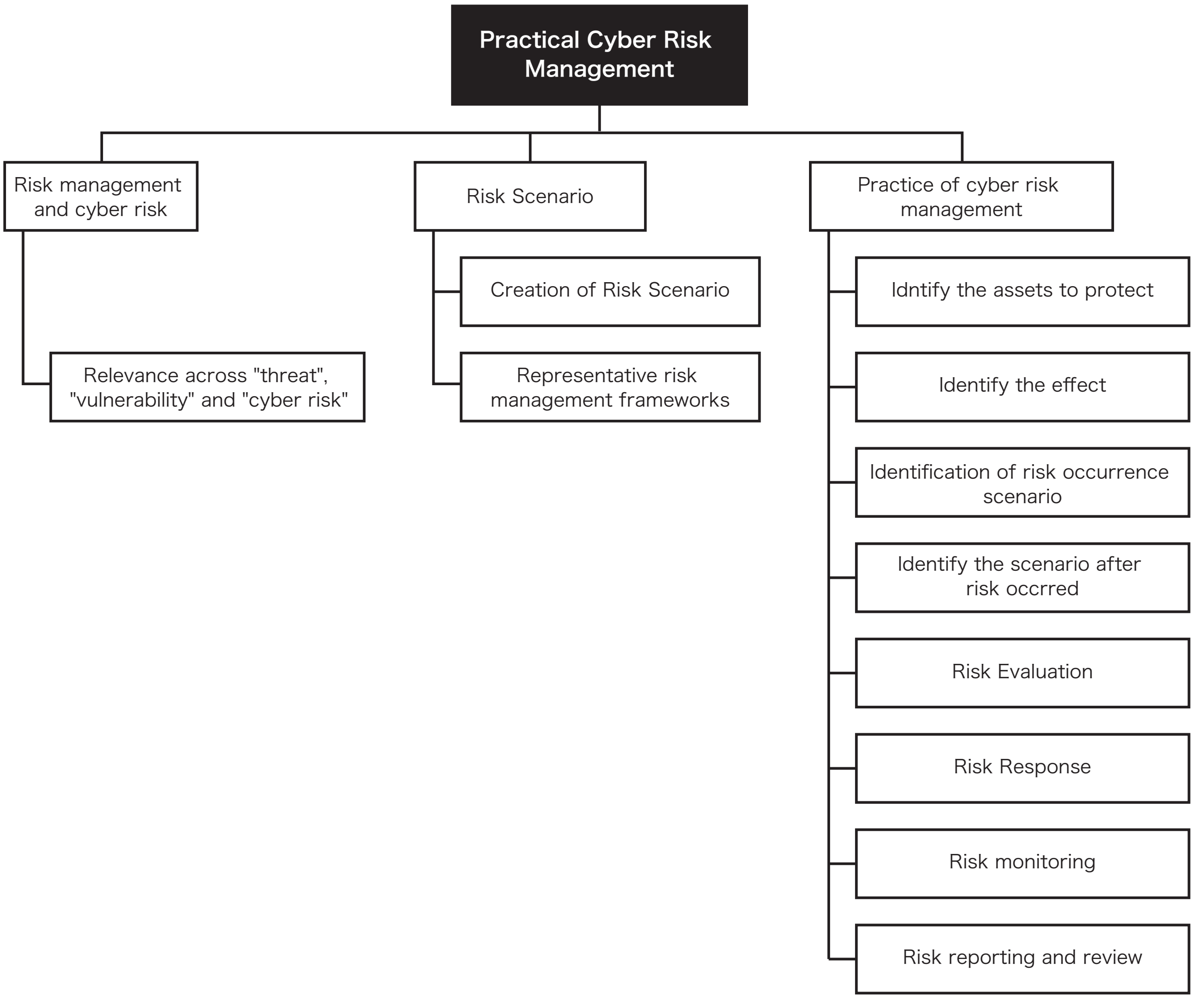

Practical Cyber Risk Management
Risk management and cyber risk
Relevance across "threat", "vulnerability" and "cyber risk"
Risk Scenario
Creation of Risk Scenario
Representative risk management frameworks
Practice of cyber risk management
Idntify the assets to protect
Identify the effect
Identification of risk occurrence scenario
Identify the scenario after risk occrred
Risk Evaluation
Risk Response
Risk monitoring
Risk reporting and review

Figure 11-1. Topic categories in the Practical Cyber Risk Management domain

What is Practical Cyber Risk Management?

Cybersecurity entails company-wide activities- not just those involving the security team- and its objectives can be defined as:

- Identifying company assets (information or the information system) and their associated risks (IDENTIFY)
- Addressing security controls to reduce risk (PROTECT)
- Detecting signs of threats as early as possible (DETECT)
- Properly responding to incidents (RESPOND)
- Minimizing (negative) impacts by proper incident response (RECOVER)

The key to achieve the objectives listed above is risk management. This chapter provides a practical approach to address effective risk management in enterprise cybersecurity activities.

Risk Management and Cyber Risk

To provide context for cyber risk management it is first essential to understand risk profiling, which is an essential underpinning of governance and management scope, goal setting, and goal alignment. The key to risk profiling is in clarifying "risk location" and "risk ownership”. All stakeholders require a common understanding of these factors to ensure business alignment.

Clarification of Risk Location

In order to make appropriate decisions and respond to risk effectively, the person who accurately understands "the value of the thing to be protected" must be the owner. The meaning of "risk management" is generally broad, and because different disciplines within an organization are intricately related, it is difficult to manage risk while aligning all perceived scopes and activities. As a result, cybersecurity activities tend to ignore correlation and causality with business impact. This is particularly true when business departments have little involvement and leave all decision-making responsibilities to IT and security departments- that have little understanding of the business. For example, a technical analysis only focusing on events like malware infection or unauthorized access without an understanding of the attacker's purpose and which organizational assets were targeted and require protection- this may lead to a flawed conclusion in the cybercrime investigation.

In addition, there may be situations where security departments or internal controls are less involved, or business departments are unable to recognize a risk- causing insufficient risk management and response. This is caused by blind spots in existing guidelines and frameworks, and often occurs in domestic companies with resource constraints and flawed governance structures.

To address these issues, the following three risk groups should be identified as "Peak Events” (the highest risk level category in a fault tree analysis) and correlated to the business, to enable more effective management and accountability:

- Information Leakage: For example, information leakage from a customer database.
- Business Obstruction: For example, the shutdown of an enterprise system.
- Financial Swindling: For example, payment to an unauthorized recipient performed by an accounting employee tricked by fraud.

Clarification of Risk Ownership

Accountability becomes more explicit when risk is defined by the association of peak events to the business. Senior and business management should be responsible for final decision-making around organizational risks, including the final assessment of risk, the implementation of countermeasures, and responses following an incident. Even if some functions supporting the business are entrusted to contractors, outsourcing partners, or the security department through agreements and defined service levels, responsibility for the impacts (to the business, customers, and partner organizations) from information leaks or service outages remains with business managers. In the case of information leakage, this would be the COO or the sales manager. In the case of business obstruction, this would be the person in charge of the business. In the case of financial swindling, this would be the head of the finance department.

Without the mapping of peak events to the business, the risk analysis workload becomes excessive and risk assessment is likely to fail. IT security often falls into this trap. Without clearly identifying personnel in charge of a given risk, it is impossible to determine the impact of the risk- leading to inefficient countermeasures and investments. Consensus is only possible when risks are related to the business and responsibility is defined.

●Relevance across “threat”, “vulnerability”, and “cyber risk”

It is important to confirm the meaning of risk, which often has vague and diverse definitions that confuse risk management-related discussions.. Risk is caused by threats such as phishing emails or exploited vulnerabilities (of systems, devices, or even people in the organization). In the case of typical ransomware incidents, extortion, data leakage, or data theft (risk) is caused by a low-literacy employee (vulnerability) opening a phishing e-mail and clicking an attachment file (threat). The following figure outlines this relationship:

Figure 11-2. Relevance across “threat”, “vulnerability” and “cyber risk”

Threat (origin)	Vulnerability	Risk
Phishing mail	Low-literacy employee	• Information leakage by malware infection • Extortion or sabotage by ransomware infection
Exploit	Unpatched System	• Information leakage by malware infection • Extortion or sabotage by ransomware infection
Malicious website	Low-literacy employee (to visit) Un-detecting security software	• Information leakage by malware infection • Extortion or sabotage by ransomware infection
Impersonated criminal	Loose access control	• EIntrusion into the network
Supplier	Immature security management for suppliers	• EInformation leakage by supplier

Threats can be categorized by their origin as either 1) intentional, 2) accidental, or 3) third-party, as shown in figure 11-6. Intentional threats can also categorized by their origin from a) an external person or group such as criminal access brokers or data brokers who attack, create a backdoor for the consequent crime, and sell stolen data to extortionists or b) an internal person or group who may be active criminals with defined objectives or passive criminals forced to commit crimes by external criminals.

Accidental threats are unintentional- a typical example is a mistake in software, processes, or IT service operation.

Threats may originate from a third party. For example, sophisticated targeted attacks may initially target the most vulnerable and interconnected supplier networks in the software supply chain to pursue a target objective of compromising an affiliated customer organization. Including the entire software supply chain in security risk management requires a significant amount of resources and time, as the supply chain is typically complex.

Insufficient asset management (including information, system, and access rights) and security audits can also introduce unknown or unidentified threats (uncategorized).

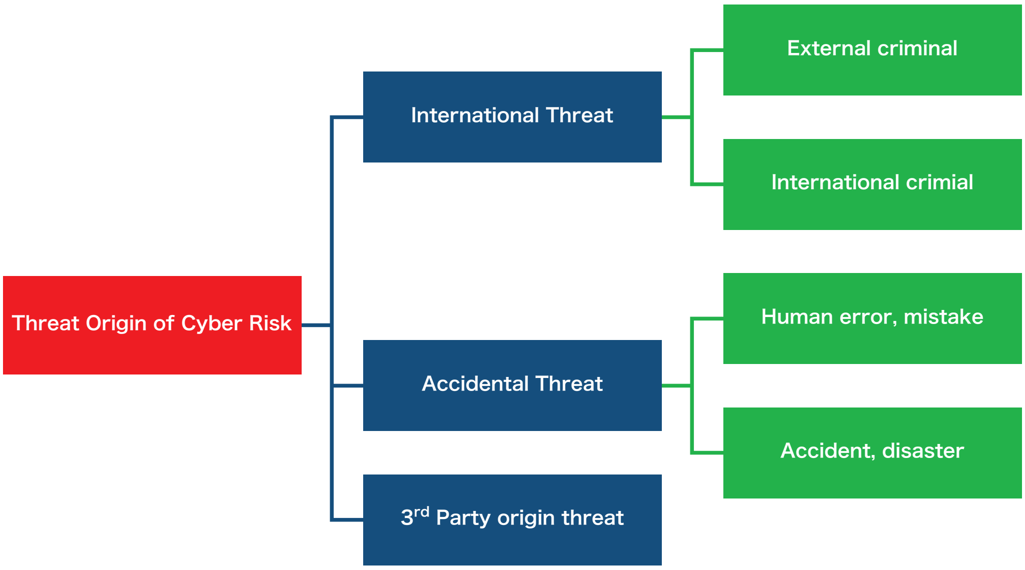


Figure 11-3. Threats of Cyber Risk

When risks become reality, negative impacts can extend beyond the victimized organization not just within cyberspace but also to the physical world. For example, the ransomware crime committed against Colonial Pipeline in 2021 disrupted gas and oil delivery throughout multiple states in the U.S. In this case, disruption of critical business operations and extortion (to pay the ransom) were the risks to the organization.

In general, risks can be categorized as:

- Information theft or disclosure
- Disruption or sabotage of business operations
- Monetary theft
- Defamation (by communication over cyberspace)
- Negative propagation of harmful ideas

Organizations should align enterprise strategy management with the potential impact of these risks, to guide investment and mitigate risk. Historically, many organizations have failed to merge cyber risk mitigation activities with business strategies. The purpose of cyber risk management is to protect not just information and systems, but also to protect the business itself. Therefore, the potential impact of risks must be linked to the business itself- making risk mitigation an investment rather than a cost.

The following application of the risk management framework will enable organizations to reflect corporate priorities in cybersecurity and CI activities. This approach allows organizations to collaborate effectively with law enforcement during investigations, protect business priorities, and enable smooth cross-team collaboration. To make this possible, organizations must first define business risks clearly and unambiguously, as will be described in the next section.

Risk Scenario

Risk management can be categorized into two major activities. The first is risk assessment, which consists of risk identification, risk analysis, and risk evaluation. The second is risk response.

Risk assessment aims to identify how a risk may happen and its magnitude if it materializes. Risk response aims to establish how to respond to a risk to reduce its impact as to an extent that the organization can accept. Together, risk assessment and risk response create the risk scenario, which is visualized by the following bow tie chart figure:

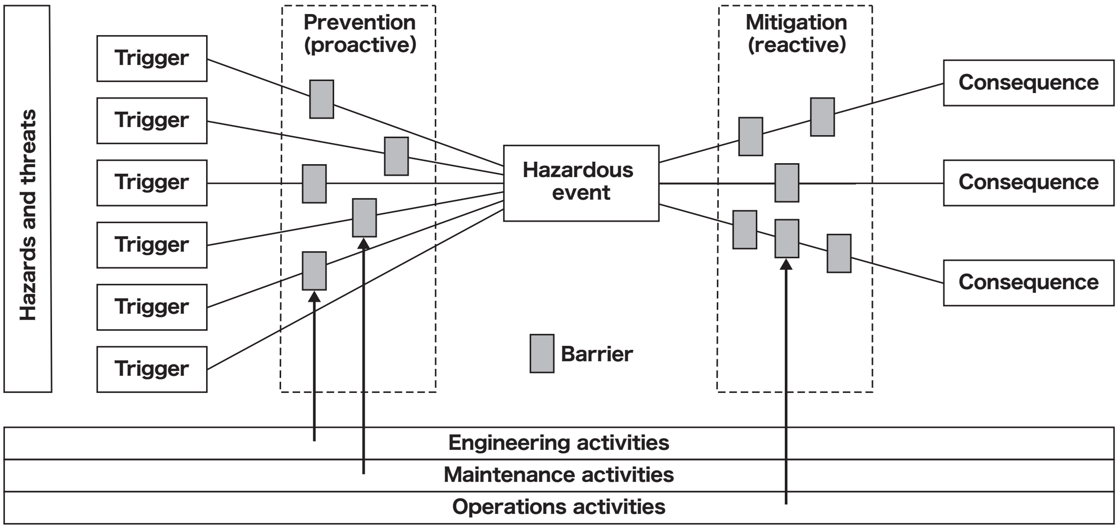


Figure 11-4. Bow Tie Chart[320]

Creating the Risk Scenario

As shown in the figure above, the risk scenario encompasses the threats which trigger proactive activities, the hazardous event itself, mitigation activities following the event, and consequences

[320] (Rausand, Marvin. - Risk Assessment: Theory, Methods, and Applications. Hoboken, NJ: John Wiley & Sons, 2011. p.120, Figure 5.3)

from the event. This approach can be applied to business continuity management (BCM) practices such that defined risk scenarios are integrated into existing corporate risk management priorities, supporting more effective resource allocation and decision-making.

However, if the chosen hazardous event is too abstract, analysis becomes ambiguous and uncertain, which in turn creates vague assessment results which are unconvincing to stakeholders. The scope of chosen events shouldn' t be too large or too small. If the scope is misadjusted or does not align with business priorities, few stakeholders will buy into the risk management process and see its value.

Therefore, risk scenarios should be created based on two frameworks. First, they should be defined around how cybercriminals actually pursue their crime objectives, divided into 4 major processes: invasion, preparation within the network, lateral movement within the network to seek the final target, and execution of the crime objective:

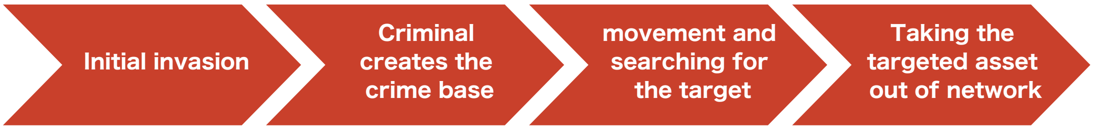

Initial invasion
Criminal creates the crime base
movement and searching for the target
Taking the targeted asset out of network

Figure 11-5. Example of crime progression scenario

In addition, risk scenarios should be created with a simplified template asking **what** will be **impacted** by **whom** and **how**:

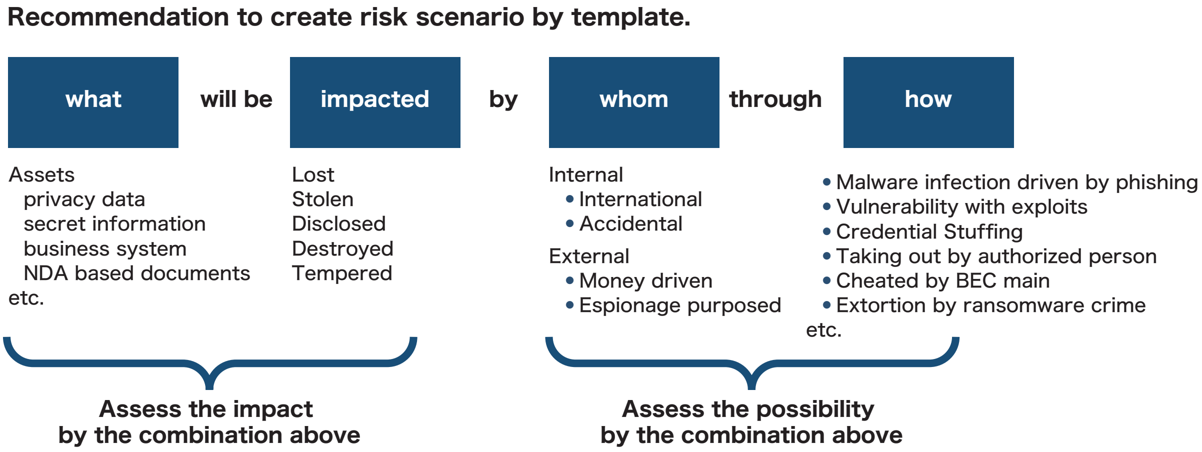

Recommendation to create risk scenario by template.
what
will be
impacted
by
whom
through
how
Assets
privacy data
secret information
business system
NDA based documents
etc.
Lost
Stolen
Disclosed
Destroyed
Tempered
Internal
• International
• Accidental
External
• Money driven
• Espionage purposed
• Malware infection driven by phishing
• Vulnerability with exploits
• Credential Stuffing
• Taking out by authorized person
• Cheated by BEC main
• Extortion by ransomware crime
etc.
Assess the impact by the combination above
Assess the possibility by the combination above

Figure 11-6. Example template to identify risk scenarios

Risk scenario identification is equivalent to "identify" in the general risk management framework which consists of identify, analyze, evaluate, respond, and monitor.

Representative risk management frameworks

After cyber risk scenario creation, a risk management framework must be chosen for alignment. Since it is often easier to apply existing frameworks, many organizations choose to utilize COBIT or IEC/ISO27001. However, these frameworks mainly focus on IT service management and must be adjusted for cyber risk management and CI activities.

Figure 11-7. Security Management Frameworks

Framework	Merit & Points for apply
IEC/ISO 27001(ISMS)	Refer to the approach to build up the holistic organization structure and management system.
NIST RMF	The framework specifically adoptive to cyber risk management lifecycle.
NIST CSF	With 5 cores and maturity model which are practically adoptive to the secury management.
NIST SP 800-171	As the supplier, verify 14 families from NIST SP 800-53 compliance.
NIST SP 800-53/ISO27002	Practical guidelines for how to implement the security control(s) divided into several families.

Figure 11-8. Risk Management Frameworks

Framework	point
ISO31000	Basic process (identification - analysis - Assessment - Response)
ISO27001/ISO27005	Annalysis ane evaluation approach specific to cybersecurity risks
NIST SP800-30	Annalysis ane evaluation approach specific to cybersecurity risks
OWASP Risk Assessment	Risk assessments specific to secure web development, etc.
Threat Modeling	A method for quantifying risk based on ISO 31000 and its method ISO 31010
NIST RMF	A model that deals with risk by focusing on information assets and information systems
STAMP/STPA/FRAM	Safety in an ecosystem consisting of a combination of complex technical areas

In the selection and adaptation of frameworks, the core consideration is simply how to best treat risk. Every organization has different assets, business priorities, and strategies. As such, risk management systems must be aligned with business needs under the guidance of C-level leadership. If different senses of value, priority, or definition exist among risk management stakeholders, risk discussions will be ineffective. A common scope, definition, goal, and framework must be established initially.

Practice of Cyber Risk Management

As previously described, cybersecurity encompasses corporate activities which:

- Identify assets that are critical to the business and its strategy, and define their risk(s)
- Address appropriate risk reduction (security controls) to protect assets
- Detect incidents and materialized risks as soon as possible
- Respond to incidents properly
- Control damages and enhance recovery

These activities must be aligned with business strategies to protect the business from cyber risks. However, most existing security guidelines around risk management are impractical- the scope focuses only on cyber risks without a consideration of business alignment, and security specialists are assigned as the lone risk management stakeholders. To implement cyber risk management into day-to-day business practices, a more practical approach is required.

Identify assets to protect

The first step in risk management is the identification of assets (information, data, or systems) which require protection. Assets must be categorized practically given constant changes to data and systems- the objective of asset identification is to protect the business itself, not each file. Categories which group assets and link them to the business structure are useful in this regard. For example, outsourcing contracts and non-disclosure agreements could be grouped under order contracts (which is a subgroup of contract documents, which is a sub-group of legal confidential information):

legal confidential information - contract document - order contract
- Outsourcing contract
- Non-disclosure agreement

A tree structure is recommended for asset categorization. Assets sharing categories should often be stored in common servers regardless of whether they are on-premises or cloud-based, as they require the same security controls (such as monitoring, access controls, and anti-malware) given their shared risk level. Once high level group categories are created, risk assessment activities are needed only for those high level categories. Organizations with extensive "shadow IT" and uncontrolled employee behavior will struggle to implement asset categorization, since employees may be able to easily store documents in unauthorized locations. Compliance and security processes must be strengthened to allow effective asset categorization.

Identify impacts

In creating an asset categorization tree structure, it is necessary to consider the impact of risks and the confidentiality, integrity, and availability (the CIA triad) of assets. Assets with different magnitudes of impact (in the case of a materialized risk) should not be categorized together. A shared definition of magnitude is necessary to avoid misalignment among stakeholders. For example:

- Large: the effect is critical to the organization (for example, business collapse)
- Moderate: the effect will damage the business and last longer than a business quarter
- Small: the effect will be recovered from within a business quarter

Definitions of magnitude should avoid personal biases and can be supported by the Existing guidelines such as FIPS 199 (Federal Information Processing Standard Publication 199), as shown below:

Figure 11-9. U.S. FIPS199 Potential Impact

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expedted to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expedted to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to send use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Identification of risk occurrence scenario

Once assets are categorized, the next step is to identify how they may be compromised- as previously explained in the Risk Scenario section. Some additional detail is provided here to guide practical risk management efforts.

●Common Scenarios

Common scenarios share key aspects and patterns. For example, if an employee' s PC is the entrance point for compromise, cyber criminals may use the PC to create a base of crime activities and expand the base for later actions (via a botnet) to exert control inside the network more easily. They may move laterally within the network to access targeted assets and steal them. In such a case, the details of the scenario may not differ much regardless of which employee' s PC is compromised. The security controls on the PC would likely be the same, as well as the network controls. The main stakeholder in defining such common scenarios should be the 2nd line of the 3 line defense model (as described in chapter 10) – security specialists.

However, there may be hidden aspects to common scenarios if, for example, an employee uses unauthorized SaaS services or IoT devices with default passwords that access the network. Therefore, the attack surface visualization (automated to some extent, if possible) is critical to pursue prior to defining common scenarios. Common scenarios should include conditions accounting for the fat that security rules may not always be followed by employees.

●Individual Scenarios

Some scenarios are individualistic and cannot be covered by common scenarios; for example, scenarios involving SaaS applications with specific uses in business sections, web servers built by marketing divisions, and factory control systems. In these cases, the 1st line team (the business section) should conduct risk assessments.

As cloud migration becomes more common and changes to business processes occur more rapidly, more individual scenarios will continue to emerge. Both regular and irregular assessment activities are necessary to limit the number of unknown individual scenarios. Regular assessments should be aligned to the PDCA cycle. Irregular assessments should be triggered by defined events, such as the identification of major vulnerabilities, major changes to organizations (people and processes) , or significant incidents or rule violations.

●Method of analysis

Templates are the final product of analyzed risk scenarios. The creation of such templates should be aided by scenario identification tools such as Fault Tree Analysis (FTA), which is used for root cause analysis and quality management (using a tree structure, sometimes called an “attack tree”). For example, in FTA, the “top event” could be data leakage of a customer database used across all business sections . Major categories beneath the top event would then be created to start in-depth analysis: for example, the top event could be caused by external criminals, internal criminals, by accident or mistake, or third parties. A sample FTA is provided below:

Deductive Reasoning (Fault Tree Analysis)

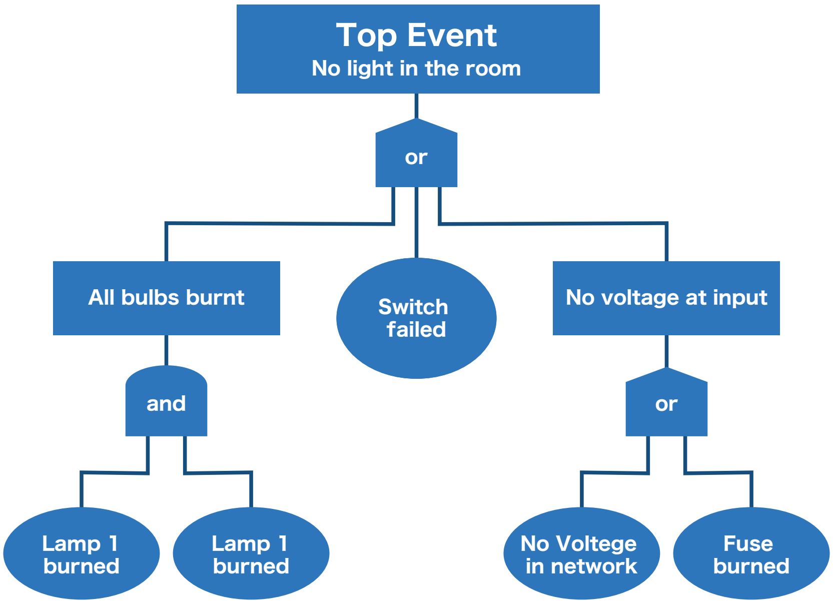


Figure 11-10. Example of Fault Tree Analysis chart

●Notable points

Cybercriminals use various methods to target networks and achieve compromises. It is critical to grasp the nuances of methodology to properly create risk scenarios. MITRE ATT&CK is a resource provided by the MITRE Corporation which documents observed cybercriminal techniques and provides enough in-depth information for most analysis. However, excessive detail requiring a high level of technical knowledge should be avoided to enable a practical approach for 2nd line security specialists that doesn' t overburden them. At the same time, as mentioned previously, too little detail must be avoided as well. A sweet spot must be achieved such that scenarios are described based upon their key aspects without too much technical detail. After all, the objective of risk management is to protect the business through efforts that are practical. For example, a risk scenario might be described as follows: the criminal will log in via a spoofed account and use legitimate tools such as VPNs to access and steal targeted data. The organization would then need to determine if such behaviors can be detected and blocked by existing controls and processes, and if not, what remedial steps are required.

Identification of the risk scenario after an incident occurs

The organization also should identify the risk scenario and how to respond once an incident occurs. Grouping is still required in this case to avoid identifying too many scenarios. The following groups are recommended as a starting point.

●Initial invasion phase

If signs of compromise can be detected at a very early stage, response scenarios will work effectively and may mitigate damages almost completely. For example, if automatic networking switching by a SDN (Software Defined Network) leads a criminal to a dummy target and the organization is able to reset access rights, data theft can be prevented. Criminals' objectives may also be identified by the monitoring of impacts. However, detecting and blocking will often be the best approach.

●Phase of activities inside the network

If a detection occurs days after a criminal has accessed a network, it is critical to identify the length of time for the invasion. This information is helpful in determining whether the criminal has already achieved their gaols. In addition, response scenarios should identify which assets have been impacted and what degree of damage has occurred (for example, breached, falsified, stolen, etc.). This aspect of investigation should be pursued prior to the clean-up of infected machines, as they contain critical artifacts for investigation. Once clean-up is conducted, it is almost impossible to collect artifacts.

For example, log data is an important artifact in many investigations. If a detection occurs and log data is lost due to clean-up activities, the organization will lack a full understanding of the incident and will be unprepared for follow-up consequences from the incident. For example, if secret information was stolen, business strategy may be impacted. If an employee with privileged access had their credentials stolen, the credentials may be used to launch an espionage attack, or to disclose sensitive information to the public and damage the organization' s reputation.

In the case of all scenarios identified after incidents have occurred, it is also important to consider how to best collaborate with law enforcement and how to communicate with stakeholders (both internal and external). Since victimized organizations can only investigate within their own networks, key artifacts in third party environments must often be investigated by law enforcement.

●Phase after data is breached

If a detection occurs after data has been breached (for example, if a company detects data theft after a ransomware group releases their stolen data to the public), it is critical to determine if the crime is still ongoing. In the example here, given the common nature of distributed crime operations and CaaS, it is possible that ransomware affiliates (including ransomware-as-a-service subscribers) may access stolen data to perpetrate additional extortion. The scope of this scenario highlights the need for an understanding of cybercriminals' organizational strategies in addition to their technical methods, to develop an effective response.

●Method to develop the response scenario

Event tree analysis (ETA) is a good tool to support the development of incident response scenarios. ETA starts with the "trigger event" and considers how the event (and its consequences) will progress, placing decision points on each consequence. For example, if the trigger event is an alert from an organization's SOC, the initial phase of response is triage to identify if an incident occurred (or not) and its associated impact. The identification of how all phases of an incident (or crime) will progress is critical for effective responses. Fortunately, event consequences tend to have certain patterns which enable organizations to learn from past incidents. As described above, there are 3 major scenario patterns based on the phase in which an incident is detected (initial invasion, activities inside the network, and after data is breached). Organizations should therefore develop three general response scenarios that correspond to the three patterns, from which more specific scenarios can be created.

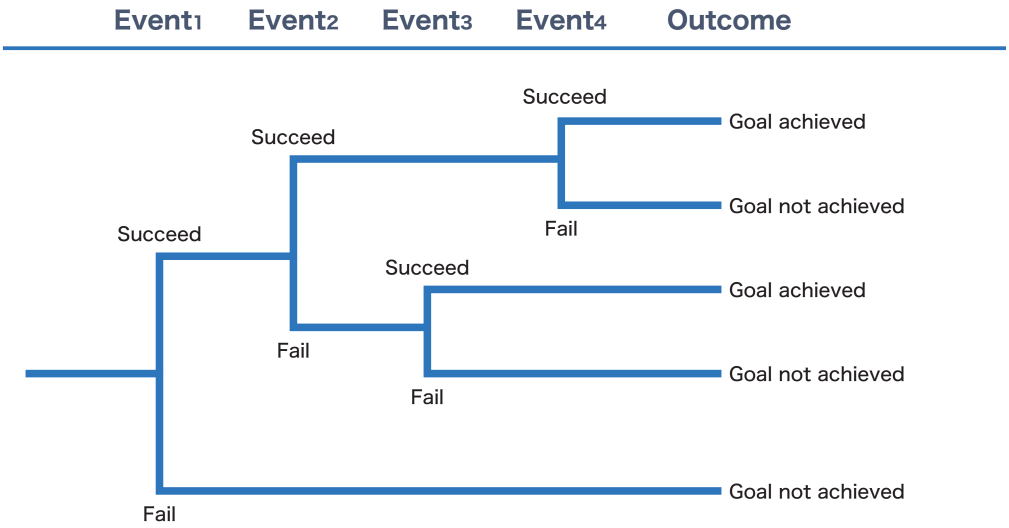


Figure 11-11. Example of Event Tree Analysis Chart

Risk Evaluation

After identifying a risk scenario, the next step is the evaluation of risk. In general risk management guidelines, risk is determined by multiplying the size of impact by likelihood of occurrence (probability) and then dividing that by the organization's ability to mitigate the risk. However, as mentioned in Chapter 10, cyber risk is not always so easily defined. For example, probability is not always easily determined when cybercriminals' behaviors are unpredictable. In addition, if a critical vulnerability is published, probability increases- proving that risk is a dynamic, not static, measure.

Regardless, risk should be calculated by the organization' s ability to prevent or mitigate the risk. If, for example, the organization has capabilities to identify risk scenarios and apply appropriate security controls (through collaboration between 1st and 2nd lines of defense, per the Three Lines Model), risk can be reduced.

● Risk value per scenario

Risk evaluation should be preceded by the identification of the occurrence scenario, as previously mentioned. However, evaluation can be pursued after security controls are implemented. The effectiveness of controls can be identified by the difference in risk value before and after their implementation.

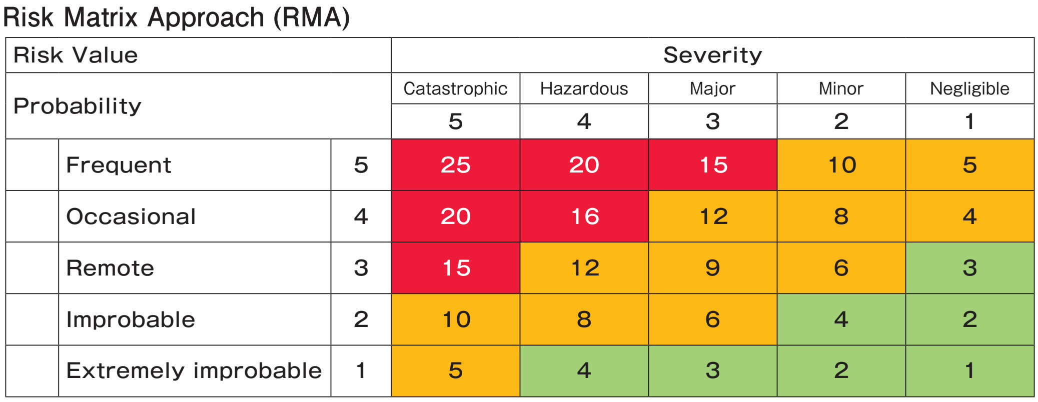
● Security controls

Many security controls will be common across organizations (such as firewalls, IDS/IPS, anti-malware software, and EDR), in terms of the associated technology, people, and process. Although common controls may not always work to mitigate asset risks by default, they can be customized to fit particular risk scenarios. This is an important step to enable cost-effective risk management. In addition, as a single control cannot typically prevent risks from occurring, the combination of controls in a layered defense is critical.

● Quantitative Evaluation

Quantitative values for risk are beneficial for a rational and scientific approach. However, quantitative values can be complex in practice. For example, if a risk reporter quantifies a risk as 80/100 but the executive they report to does not understand scores on the 100 point scale (meaning, it does not convey a common value), the quantification is not useful. Before utilizing quantitative values, it is necessary to develop a common understanding of the indicator system. The risk matrix approach shown below is a well-known and commonly adapted system for qualitatively valuing risks:

Figure 11-12. Example of a risk matrix for qualitative assessment



Risk Matrix Approach (RMA)

Risk Value			Severity				
Probability			Catastrophic	Hazardous	Major	Minor	Negligible
			5	4	3	2	1
	Frequent	5	25	20	15	10	5
	Occasional	4	20	16	12	8	4
	Remote	3	15	12	9	6	3
	Improbable	2	10	8	6	4	2
	Extremely improbable	1	5	4	3	2	1

Once an organization is mature enough to conduct comprehensive risk management, aforementioned tools such as fault tree analysis (FTA) and event tree analysis (ETA) can be integrated with quantitative risk evaluations. However, cyber risks will always have a human factor, and as such quantitative indicators are best used in evaluating the effectiveness of security controls, and not in determining if an organization will be targeted.

In the ETA example below, the phishing email is the trigger event: the tree describes the likelihood of the email being blocked at the email gateway, then the likelihood of the recipient opening the email, then the likelihood of the recipient opening the attachment, then the likelihood of security software to detect and block the threat. This is a helpful approach to identifying vulnerabilities and weaknesses in an organization' s security controls.

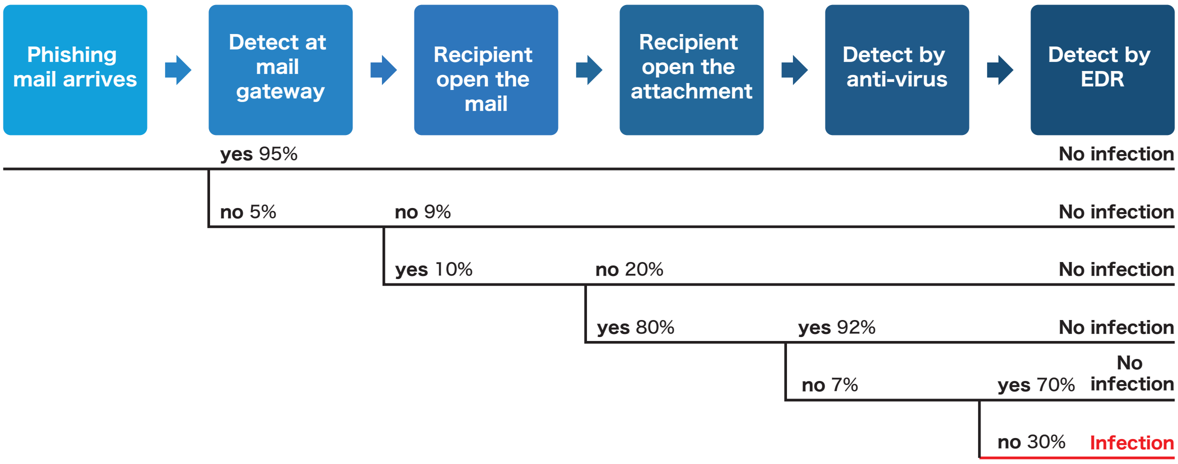
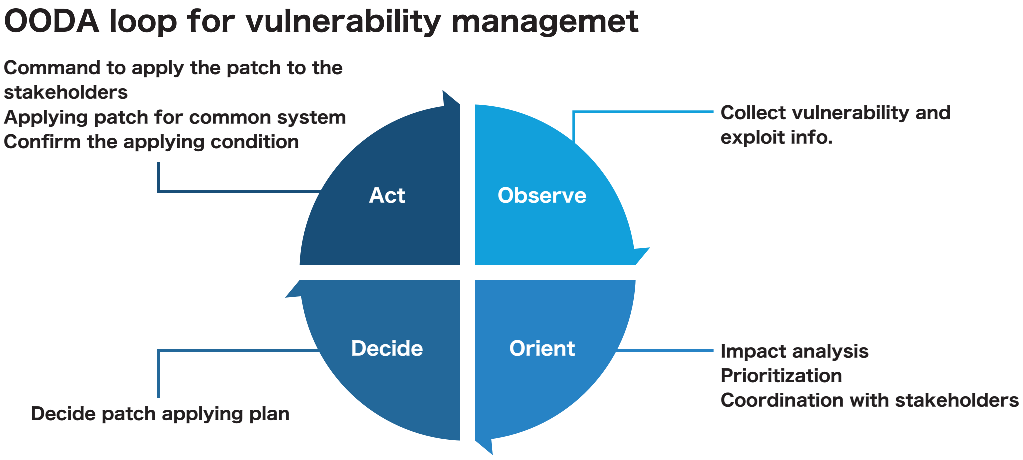


Figure 11-13. Analysis of crime success probability using event tree

●Handling vulnerabilities

Some existing cybersecurity risk management guidelines recommend accounting for vulnerabilities. However, since vulnerabilities may not be detected or may dynamically change, it is not always practical to consider them in risk evaluations. Rather than using the PDCA cycle for vulnerability information, the OODA loop proves more useful, as it is a shorter cycle that enables immediate action. This enables risk evaluation to be pursued without the full understanding of a vulnerability (or vulnerabilities) affecting relevant systems or assets; OODA allows security operations to evaluate risk quickly and make decision (like shutting down a system or patching software).



OODA loop for vulnerability managemet
Command to apply the patch to the stakeholders
Applying patch for common system
Confirm the applying condition
Act
Observe
Collect vulnerability and exploit info.
Decide
Orient
Impact analysis
Prioritization
Coordination with stakeholders
Decide patch applying plan

Figure 11-14. OODA loop for vulnerability response

Risk Response

After risk assessment (identification of the scenario/occurrence, establishment of response, and evaluation of risk), risk response must be determined. There are four choices in risk response: 1) remove, 2) reduce, 3) transfer, and 4) accept. As mentioned previously, controls can reduce but not remove risks, and victims cannot fully transfer risks to third parties. The figure below outlines the four types of risk response as they relate to probability and impact:

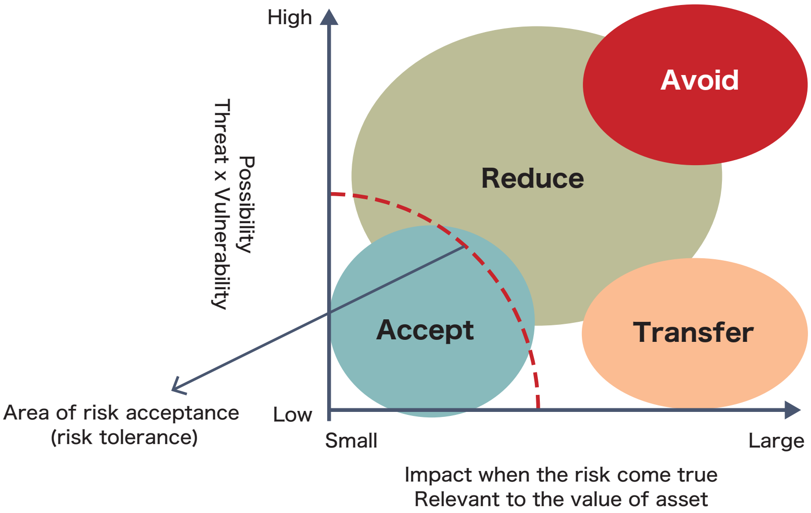


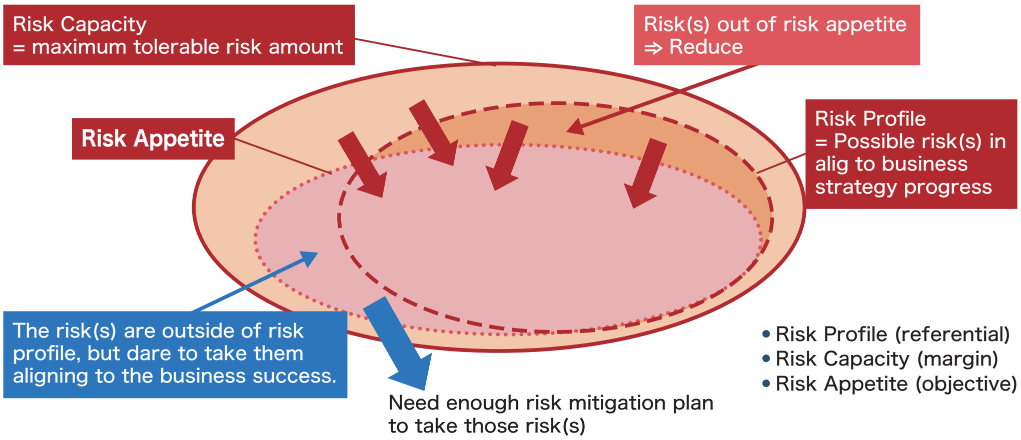
Figure 11-15. Options for risk response

Decisions around risk response should involve accountable business stakeholders, as they involve considerations of costs (from risk reduction or acceptance, delays to project schedules, etc.). In addition, if accountable stakeholders are unable to rationalize decisions, in the case that they end up being wrong, their lack of understanding behind the decisions can do additional damage (to brand reputation, etc.). Therefore, decision-makers should be the owners of assets (information, data, or systems) on business teams - the 1st line- while the 2nd line (security specialists, risk management teams) should support decision-makers’ decisions by providing relevant information. If decision-makers are on the security team, it is unlikely that they will accept risks and the cost for risk reduction will increase, subsequently delaying projects as more security controls are implemented.

The following terminology can help support decision-makers navigating risk management:

- **Risk Capacity**: The maximum risk an organization can hold in terms of cost, resources, or support required from internal/external parties. For example, if funds are available to cover costs of a risk, it may be acceptable. However, it is difficult to identify the impact of risks quantitatively and decisions based on risk capacity alone are not recommended.
- **Risk Profile**: The total amount of risk to an organization in the course of business, including cyber risks and any other type of risk, such as disaster risks and people risks. Risk profile requires that qualitative risks are translated quantitatively; for example, how much money is required to respond to a business disruption from ransomware.
- **Risk Appetite**: The amount of risk an organization is willing to take on, in alignment with business objectives. For example, if there is a tight timeline to meet a release date for an application which is currently in development and has some bugs which may have a massive

impact on users, business stakeholders determine whether to release the application on time based on an acceptable amount of risk. In this case, the organization may implement a mitigation plan to fix the bugs soon after release with automatic patching, minimizing the risk period. Risk appetite must be considered both in terms of business and security perspectives.



Risk Capacity
= maximum tolerable risk amount
Risk(s) out of risk appetite
⇒ Reduce
Risk Appetite
Risk Profile
= Possible risk(s) in
alig to business
strategy progress
The risk(s) are outside of risk
profile, but dare to take them
aligning to the business success.
Need enough risk mitigation plan
to take those risk(s)
• Risk Profile (referential)
• Risk Capacity (margin)
• Risk Appetite (objective)

Figure 11-16. Relationship between risk profile, capacity, and appetite

- **Risk Tolerance**: The maximum acceptable risk an organization is willing to take on according to its policies, strategic objectives, and standards aligned with security objectives. Risk tolerance is a critical benchmark to guide risk management decision-making. Maturity in risk management is required to establish risk tolerance.
- **ALARP (As Low As Reasonably Practicable)**: A concept describing the level to which risks must be reduced. ALARP is reached when the cost of risk reduction is disproportionately higher than the continued reduction of a risk' s impact, and is particularly applicable to moderate risks which are neither intolerable or fully tolerable. Using a simplified example, if a system will earn $100 and the cost to reduce the risk to the system is also $100, the benefit of doing so is zero and risk reduction steps may not be taken. ALARP provides a helpful framework to explain how and why an organization made particular risk management decisions.

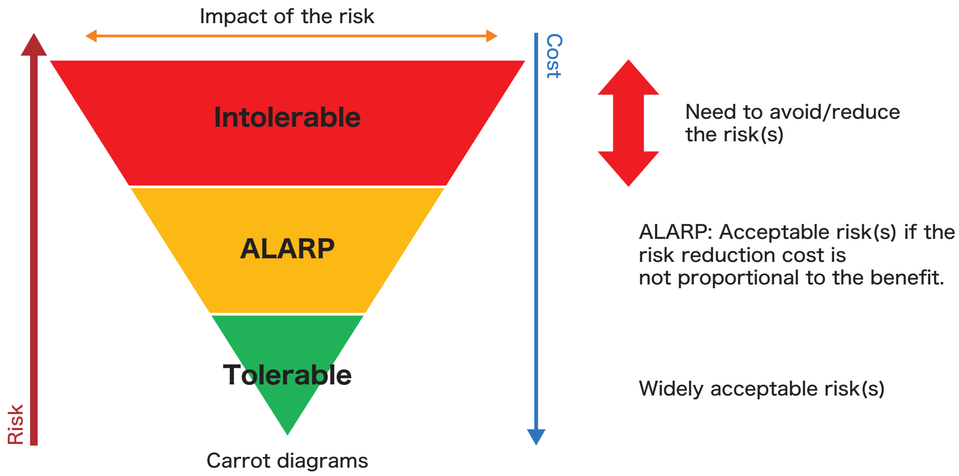


Figure 11-17. ALARP

A cost-benefit analysis (CBA) can be used to determine ALARP by identifying the point at which the cost of risk reduction meets the cost of risk. Quantitative risk evaluation must be utilized to apply a CBA in this manner.

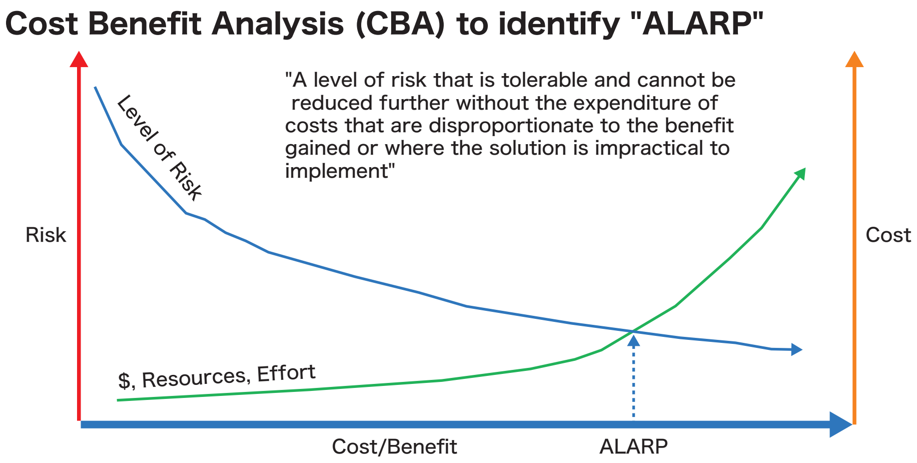


Figure 11-18. Calculating ALARP using cost-effectiveness analysis

Risk monitoring

The last phase of risk management is the monitoring of risk levels (and whether they are acceptable) to confirm the effectiveness of risk reduction actions. This phase is critical in demonstrating the value of risk reductions. Risk monitoring is equivalent to the “Check” phase in the PDCA cycle.

It is critical to note that changes which affect an evaluated risk scenario often occur and raise the level of risk; for example, if new malicious tools are found to target a company operations system containing key assets. This creates a situation in which risk levels are higher than when the initial risk evaluation was completed. As such, risk monitoring should be conducted periodically (before, during, and after risk reduction actions) to inform a real-time risk dashboard system which visualizes changing levels of risk.

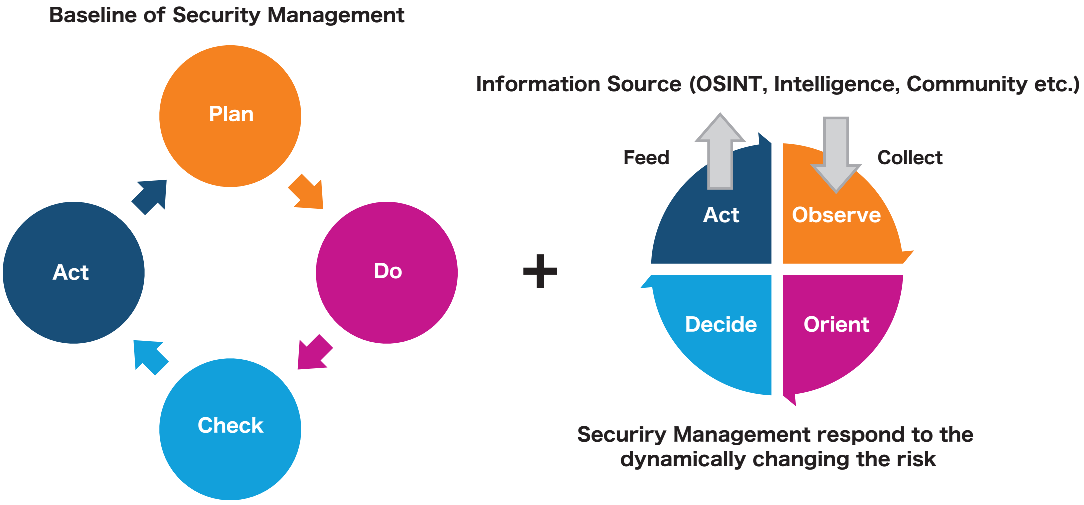

Baseline of Security Management
Plan
Do
Check
Act
+
Information Source (OSINT, Intelligence, Community etc.)
Feed
Collect
Act
Observe
Decide
Orient
Securiry Management respond to the dynamically changing the risk

Figure 11-19. Cyber Security PDCA + OODA

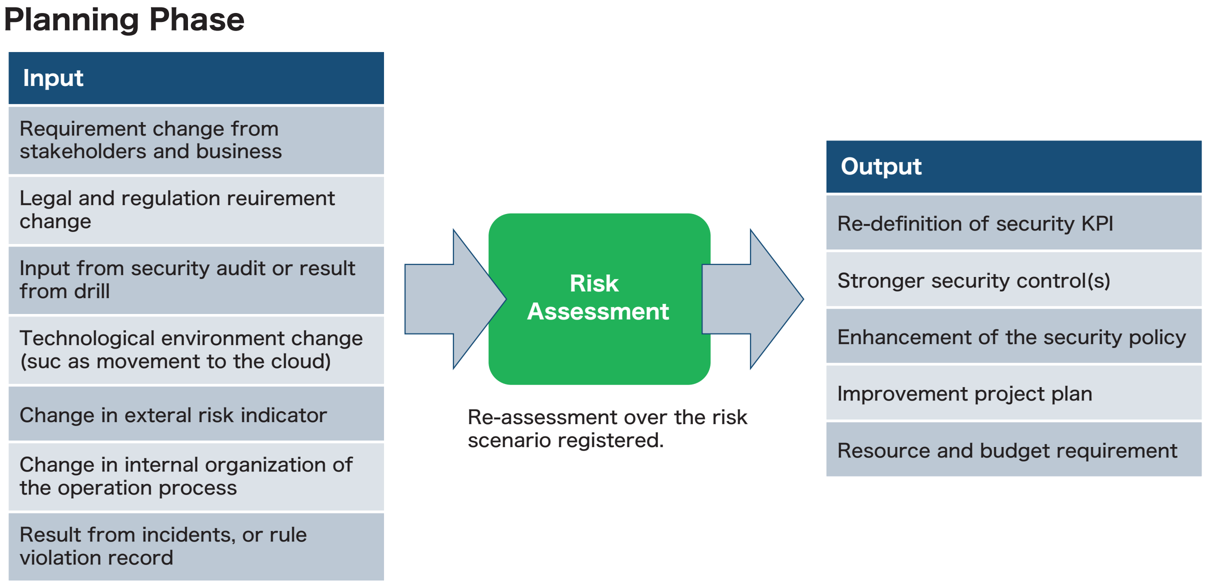

Planning Phase
Input
Requirement change from stakeholders and business
Legal and regulation reuirement change
Input from security audit or result from drill
Technological environment change (suc as movement to the cloud)
Change in exteral risk indicator
Change in internal organization of the operation process
Result from incidents, or rule violation record
Risk Assessment
Re-assessment over the risk scenario registered.
Output
Re-definition of security KPI
Stronger security control(s)
Enhancement of the security policy
Improvement project plan
Resource and budget requirement

Figure 11-20. Example of risk reassessment input

Triggers to re-evaluate (reassess) risk levels should be utilized to best capture the dynamic nature of risks. Triggers may include:

- If the risk impact (ex: CIA triad) changes
- If a security incident occurs
- If a large scale vulnerability is reported
- If a large organizational change or role change occurs
- If a major system change is implemented
- If a major business operations process change occurs
- If a legal regulation or government requirement goes into effect

Risk reporting and review

A visualization system to check the progress, effectiveness, and employee objectives around risk management is critical. However, many organizations face challenges in communicating the results of risk management to business and executive stakeholders. Some of the most common challenges include:

1. Executives don’ t understand the security team’ s reporting
2. Risk reporting is not discussed at board meetings
3. Risk scenario reviews are not conducted upon business environment changes (despite frequent and rapid changes)

CISOs (Chief Information Security Officers) play a key role in solving these problems. Organizational and business requirements should be taken into account by the CISO and used to interpret security reporting for executive and business audiences. KPIs should be developed for security related activities (regardless of the responsible team(s)) and aligned with high level business needs to avoid standalone/passive cybersecurity activities. CISO should also help board members verify if executive managers are making good decisions- a critical aspect of proper risk governance.

Maturity models are an additional consideration which can aid in risk management communications. For example, NIST' s Cybersecurity Framework (National Institute of Standards and Technology - NIST CSF[321] for critical infrastructure companies and the CMMC (Cybersecurity Maturity Model Certification) framework[322] developed by the U.S. Department of Defense both recommend maturity models to evaluate the security level of an organization. Notably, both models focus on how organizations manage cybersecurity, not how they identify risks in detail. Risk visualization and review can be strengthened with the combination of a maturity model and risk scenario assessment.

The following tactics can help CISOs communicate risk reporting and reviews more effectively to executives:

1. Instead of "malware infection risk" (which is just one piece of risk impacts), "information leakage by malware infection" (emphasizing what will happen to the business and its impact) should be reported.
2. Understandable and business aligned risk indicators like "cost" and "resources required" should be used to communicate the quantitative value of risks. In addition, security KPIs should be implemented into BSC (balanced scorecard) and other performance management frameworks.
3. Reports to executives should be conducted regularly (as frequently as monthly and at least quarterly). Reports should, in addition to explaining risks, create dialogue around what is needed from executives and required for security.

[321] https://www.nist.gov/cyberframework

[322] https://dodcio.defense.gov/CMMC/About/

Chapter 11: Association to the CIBOK Taxonomy

As previously described, the execution framework of the CIBOK Taxonomy details the inter-relationship between knowledge domains necessary to understanding the functions and utility of cyber investigation in an organization. The process of investigating a cybercrime depends upon a determination of the type of, available sources of evidence according to the scope of the crime (and related artifacts), and is supported by practical methods of evidence collection and analysis. Responsible information sharing between victims and public and private sector organizations helps an organization to resolve cybercrime incidents.

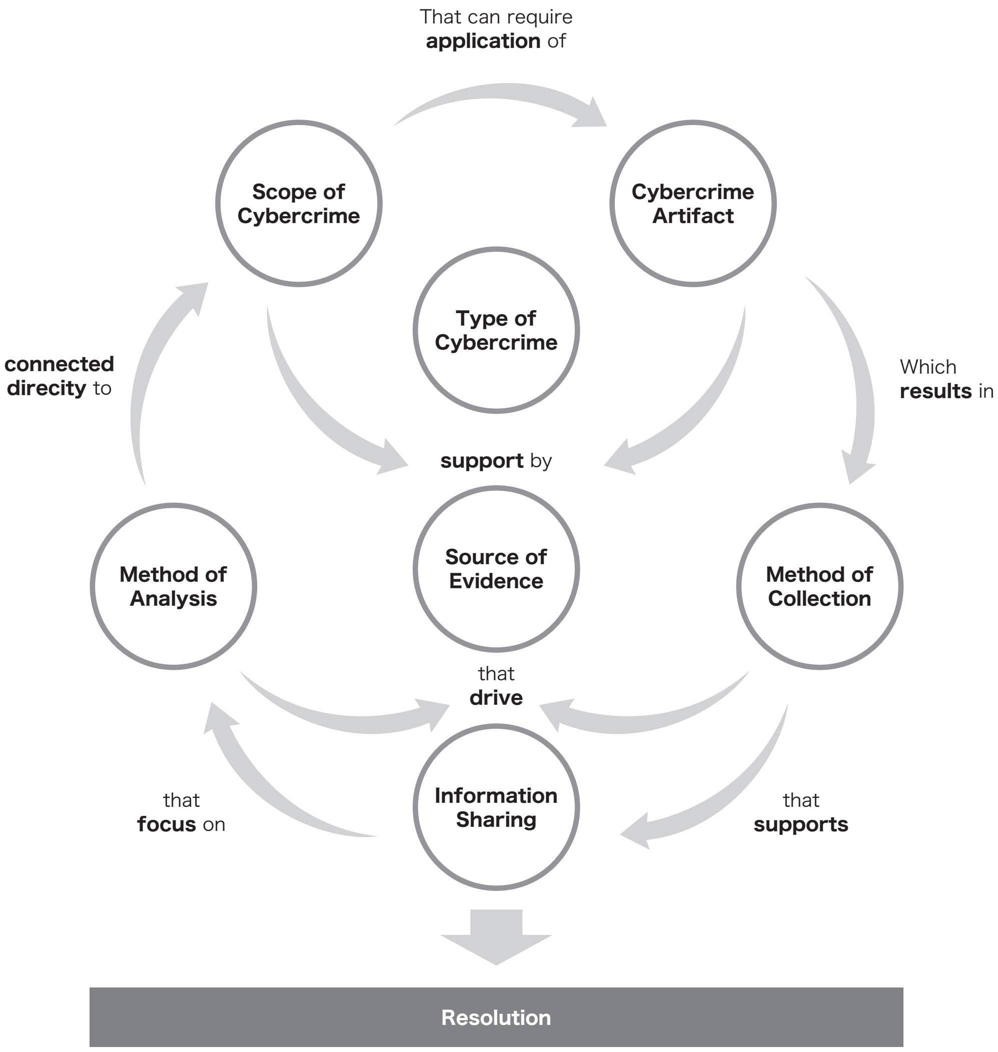


Figure 11-21. Cybercrime Investigative Execution Framework

The relationship between the execution framework and the CIBOK taxonomy of skills and knowledge (see Appendix A) demonstrates that the functional requirements vary across related roles.

Figure 11-22. CIBOK Taxonomy

	Required Skills and Experience						
CIBOK Framework	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	H	H	H	H	L	L	N/A
Description of Cybercrime	H	H	H	H	H	L	L
Objectives of Cybercrime	H	H	H	H	H	L	L
Cybercriminal Profiles	H	H	H	H	H	N/A	N/A
Cybercriminal Organizations	H	H	H	H	H	N/A	N/A
Indicators	H	H	H	L	L	L	N/A
Stages	H	H	H	M	M	L	N/A
Artifacts	M	H	H	N/A	N/A	L	N/A
Scope	M	H	H	M	M	L	N/A
Sources of Evidence	M	H	H	M	N/A	L	N/A
Methods of Evidence Collection	M	H	H	M	N/A	L	L
Methods of Evidence Analysis	M	H	H	M	N/A	L	L
Resolution	H	M	H	M	M	L	L
Cybercrime Information Sharing	M	H	H	H	H	L	L
Management Framework	H	L	M	L	L	L	M

Figure 11-23. CI Execution Framework association to CIBOK Taxonomy

	Executive	Intelligence	Investigation	Judiciary	Public Relations	Support	Administrative
Cybercrime Investigation	S	T	T	S	T	P	P
Type of Cybercrime	S	T	T	S	S	T	P
Cybercrime Artifact	S	T	T	T	P	T	P
Scope of Cybercrime	S	T	T	S	T	T	P
Scope of Evidence	S	T	T	T	P	T	P
Methods of Collection	S	T	T	P	P	T	P
Methods of Analysis	S	T	T	P	P	T	P
Resolution	S	T	T	S	T	P	P
Information Sharing	S	P	P	T	T	P	T
Management	S	P	P	P	P	P	T

< legend >
S : Strategic
T : Tactical
P : Procedural

Executive – require strategic understanding of the procedures and policies concerning cybercrime investigation and the description of cybercrimes being investigated. This includes the related objectives, scope, and sources of evidence concerning the crime in its apparent stage of execution (or achieved goals). The executive function describes for the organization the nature and types of cybercrime. The executive function should develop policies, procedures, and plans – and manage the (human and other) resources and their continuing development.

Intelligence – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to available sources of evidence. This function assists the investigative, judiciary, public relations, and executive roles in comprehending risks (from evidence or analysis of information and market sentiment) to the victim. Intelligence is a crucial source of information for determining the nature, scope, and objectives of cybercrimes according to available evidence. Intelligence staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Investigative – require tactical and procedural understanding of the scope and impact of cybercrime(s) according to artifacts and evidence in available sources. This function assists the intelligence, judiciary, public relations, and executive roles in qualifying the impact of cybercrime according to assessed nature (and stage of achievement) of related goals. Investigations staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Judiciary – require strategic understanding of the jurisdictional and procedural allowances and limitations of the investigative process. This function assists the executive and public relations roles by guiding intelligence collection, investigative procedures, and interpreting the results of analysis according to laws, regulations, and associated policies. Regulatory and statutory guidance will provide restrictions and penalties for the sharing of information. Senior staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Public Relations – require strategic understanding of the types, objectives, profiles and structure of cybercrimes and their organizations. This function also requires strategic understanding of venues and methods of information sharing for responsible disclosure. The scope of cybercrime discovered through investigation and analysis will determine, according to policy, what to communicate – with whom, and when, according to which organization/functions/personnel are affected. Senior staff should understand procedures and follow organizational policies. Senior staff should assist junior staff with developing skills and knowledge.

Support – require procedural understanding of the scope and methods of investigating cybercrimes to assist intelligence and investigative efforts.

Administrative – require procedural understanding investigative intents and organizational capabilities to collect and analyze evidence.

Chapter 11: Review

1. How should assets requiring protection be identified?

   Answer: asset categorization

   Examples: tree structure

2. Who is responsible for defining risk scenarios?

   Answer: 1st line/business section (individual), 2nd line/security specialists (common)

   Examples: Through the use of fault tree analysis or event tree analysis (following an incident)

3. How should the effectiveness of risk controls be measured?

   Answer: quantitative evaluation

   Examples: risk matrix approach

4. How is the level of investment required for risk reduction decided upon?

   Answer: ALARP

   Examples: using a cost-benefit analysis (CBA)

5. What are common triggers for the reassessment of risk scenarios?

   Answer: anything that changes risk levels

   Examples: risk impact change, security incident, vulnerability, organizational or role change, system change, business operations change, regulatory change

6. When should risk assessment results be reported to executives ?

   Answer: at least quarterly, as frequently as monthly

   Examples: CISOs using security KPIs aligned with business needs and helping boards evaluate risk management decision-making (risk governance)

Case Study 11: Insider Data Theft

- **Crime**: Data theft, Corporate Espionage
- **Suspect(s)**: Employee
- **Means**: Misuse of authorized access
- **Motive**: Personal gain
- **Opportunity**: Inadequate asset security

A senior research scientist at a leading pharmaceutical company, decided to accept an offer from a competitor. With an extensive background in pharmaceutical research and development, he had access to sensitive and proprietary information, including formulae, FDA filings, and grant information crucial to his employer's success. His departure, while supported by his coworkers, took a sinister turn that left the company grappling with the ramifications of corporate espionage.

Upon deciding to join the competitor, the research scientist initiated a series of actions that constituted a severe breach of corporate confidentiality and ethical standards. Over a period of two months before formally announcing his resignation, he accessed and transferred proprietary documents to his personal cloud storage account. The information included:

- Detailed pharmaceutical formulae under development.
- FDA filings critical to his employer's market strategy.
- Grants information and research data.

Additionally, he forwarded hundreds of internal emails containing sensitive discussions and strategic plans from his work account to his personal email. Such emails included collaborative discussions, meeting notes, and confidential correspondences that revealed proprietary research intentions and business tactics. An investigation into these activities revealed the following:

1. **Access to Sensitive Documents**: Using his credentials, he systematically gathered confidential information over several weeks. His credentials provided unregulated access to information throughout the organization due to inadequate data controls.
2. **Data Transfer to Personal Cloud Storage**: he uploaded the sensitive documents to his personal cloud storage account using his work laptop, thereby creating a repository of his employer's proprietary information accessible from anywhere.
3. **Email Forwarding**: he forwarded hundreds of work-related emails to his personal email account. This move was particularly damaging as it included not only documents but also critical internal discussions and plans.
4. **Data Deletion Attempts**: Prior to returning his company-issued laptop, he attempted to cover his tracks. He deleted his browsing history and used a free data wiper software to erase his user history, hoping to eliminate evidence of his activities.

The employer's IT department, utilizing routine HR protocols, discovered anomalies within the research scientist's data usage logs during his final days with the company. Suspicious of these activities, the team conducted a thorough forensic investigation with the support of an external consultant, which revealed the extent of his actions.

Forensic Analysis Findings:

- **Restoration of Deleted Data**: Despite his efforts, the IT team successfully restored deleted files and retrieved logs that indicated extensive data transfers to external sources.
- **Detection of Cloud Storage Access**: Logs showed repeated access to external cloud storage services, aligning with the timeline of data exfiltration. Examination of the corporate cloud data access logs also described additional devices that his credentials had been used with to download information from an IP address discovered to be related to the competitor to whom he was moving.
- **Email Forwarding Patterns**: Email server logs demonstrated suspicious forwarding patterns of emails to his personal account.

The actions taken by the former employee represent a severe breach of ethical standards and contractual obligations to maintain confidentiality. Such behavior highlights significant legal implications, including:

1. **Breach of Non-Disclosure Agreements (NDAs)**: the employee's actions directly violated his NDA and employment agreements, which explicitly forbade the transfer or disclosure of confidential information to unauthorized parties.
2. **Corporate Espionage**: Deliberate transfer of proprietary information to a competitor as a systematic attempt to undermine his employer's competitive edge constitutes corporate espionage, carrying severe legal penalties.
3. **Intellectual Property Violation**: By appropriating pharmaceutical formulae and FDA filings, he breached intellectual property laws designed to protect the original creations of the company's research and development efforts.

Faced with the considerable risk posed by the former research scientist's actions, the company initiated several responses:

- **Immediate Legal Action**: the company pursued legal remedies against the former employee for breach of contract, computer fraud and abuse, corporate espionage, and intellectual property theft. This included seeking injunctive relief to prevent his new employer from utilizing the stolen information.
- **Enhanced Security Measures**: the company reviewed and tightened its data access protocols, instituting stricter access controls, data monitoring, and multi-factor authentication processes to safeguard against future abuses of trust.
- **Notification to Regulatory Bodies**: the company informed relevant regulatory authorities of the breach, ensuring compliance with legal obligations and transparency in reporting potential impacts on public health and market practices.

This case underscores the critical importance of safeguarding sensitive corporate information, especially during employee transitions. It serves as a stark reminder for organizations to maintain vigilance through robust security protocols, continuous monitoring, and swift response action to mitigate risks associated with corporate espionage and insider threats.

Appendices

Key Terms and Definitions

Access controls—Measures that establish privileges, determine authorized access, and prevent unauthorized access.

Active digital footprint—Created by data provided by the user of a computing device or application.

Advanced fee fraud—A computer-related fraud involving a request for an advance fee to complete a transfer, deposit or other transaction in exchange for a larger sum of money.

Advanced persistent threats (APTs)—Individuals and/or groups that persistently target an entity.

Anonymity—The shielding of one' s identity to enable individuals to engage in activities without revealing themselves and/or their actions to others.

Anonymizers—These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as anonymous proxy servers.

Anonymous proxy servers—These proxy servers enable users to hide identity data by masking their IP address and substituting it with a different IP address. Also known as anonymizers.

Anti-digital forensics—Tools and techniques used to obfuscate cybercrime investigation and digital forensics efforts. Also known as antiforensics.

Appellations of origin—Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as geographical indications.

Application and file analysis—Type of analysis that is performed to examine applications and files on a computer system to determine the perpetrator' s knowledge of and intent and capabilities to commit cybercrime.

Artifacts—traces and clues that reflect the planning, organization, conduct, and commission of cybercrime.

Asset—Something that is considered important and/or valuable.

Attribution—The determination of who and/or what is responsible for a cybercrime.

Attribution profiles—information about criminals or the preliminary groups from which they are recruited.

Automation—the use of computers to perform analysis on data of such volume that it cannot be performed manually, using a variety of analytical frameworks, and to carry out analysis from different viewpoints.

Availability—Data, services, and systems are accessible on demand.

Backdoor—A secret portal used to gain unauthorized access to systems.

Back-tracing—The process of tracing illicit acts back to the source of the cybercrime. Also known as traceback.

Best evidence—The original piece of evidence or an accurate duplicate of the original.

Big data—large volumes of structured and unstructured data that can be consolidated and analyzed to reveal information about associations, patterns, and trends.

Black-Hat hackers—hackers that gain unauthorized access in order to steal credit card numbers or Personally Identifiable Information (PII) for identity theft; seek personal gain, financial or otherwise, and to raise havoc in some cases; use DDoS attacks and code malware; and are very skilled in hacker techniques and getting past security systems in networks.

Botherder—Controller of bot-infected digital devices.

Botnet—a group or network of bots under the control of the same attacker.

Bot—type of malware that an attacker can use to control an infected computer or mobile device.

Brute force attack—The use of a script or bot to guess user credentials.

Bulletproof hosting—A service that enables criminals to utilize servers to commit cybercrime, store illicit content, and protect illicit content from being accessed by law enforcement authorities and/or being taken offline.

Business continuity plan—Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as emergency management plan.

Catphishing—False or misleading promises of love and companionship designed to scam individuals out of their time, money and/or other items.

Censorship—The prohibition of information, visual depictions, and written or oral communications that are prohibited by law and/or their suppression by a government, community, or group because they are unlawful and/or viewed as harmful, unpopular, undesirable, or politically incorrect.

Chain of custody—A detailed log about the evidence, the condition of the evidence, its collection, storage, access, and transfer and reasons for its access and transfer, is essential to ensure the admissibility of digital evidence in most courts of law.

Child grooming—Enticement of children or solicitation of children for sexual purposes.

Child sex trafficking—Acting in some manner that recruits, leads, causes, maintains, and/or otherwise facilitates the commercial sexual exploitation of children.

Child sexual abuse material (CSAM)—The representation of child sexual abuse and/or other sexualized acts using children.

Child sexual abuse to order—Viewers of child sexual abuse can be actively involved in abuse by communicating with the child, the sexual abuser, and/or facilitator of the child sexual abuse and requesting specific physical acts and/or sexual acts to be performed on and/or performed by the child.

Circumstantial evidence—Evidence that infers the truth of a matter.

Clearnet—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Surface Web or Visible Web.

Clou—internet hosted servers that provide virtualized computing and storage services and resources.

Code of ethics—Guidelines covering right and wrong conduct to inform decision-making.

Collected evidence—the collection of a foundation to identify an individual or organization that has committed a wrongful act or participated in the act.

Commercial sexual exploitation of children—A term used to describe a range of activities and crimes that involve the sexual abuse of children for some kind of remuneration of any monetary or non-monetary value.

Computer data—Any form of representation of information that is processed by a system of a digital device. Also known as computer information or data.

Computer Emergency Response Team—A team that provides support for cybersecurity incidents. Also known as Computer Security Incident Response Team.

Computer information—Any form of representation of information that is processed by a system of a digital device. Also known as computer data or data.

Computer network—Two or more computers that send and receive data between them.

Computer Security Incident Response Team (CSIRT)—A team that provides support for cybersecurity incidents. Also known as Computer Emergency Response Team.

Computer system—A stand-alone or networked device that performs data processing among other functions.

Confidentiality—Systems, networks, and data are protected, and only authorized users can access them.

Confirmation bias—The process whereby individuals look for and support results that support their working hypothesis and dismiss results that conflict with their working hypothesis.

Content data—Words in written communications or spoken words.

Coordinated vulnerability disclosure—The practice of harmonized information sharing and disclosure of vulnerabilities to relevant stakeholders along with the tactics used for its mitigation.

Copyrights—Creative products, such as artistic and literary works, protected by law.

Crime displacement—When a crime that was intended for one target is committed on another target because of security measures in place.

Crime reconstruction—This process seeks to determine who was responsible for the crime, what happened, where did the crime occur, when did the crime take place, and how the crime unfolded, through the identification, collation, and linkage of data. Also known as event reconstruction.

Crime scene indicators—elements that comprise a crime scene.

Crimeware—general term for software created or used for criminal acts.

Critical infrastructure—Designated essential sectors that are considered fundamental to the proper functioning of society.

Cryptocurrency—A form of digital currency secured utilizing advanced encryption.

Cryptomarkets—A website utilizing cryptography to protect users of the site.

Crytopjacking—A tactic whereby the processing power of infected computers is used to mine cryptocurrency for the financial benefit of the person (or persons) controlling the bot-infected digital devices.

Cyber organized crime—A term used to describe a continuing criminal enterprise that rationally works to profit from illicit activities that are in demand online.

Cyber organized criminals—A structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the United Nations Convention against Transnational Organized Crime of 2000, which operate in whole or in part online, in order to obtain, directly or indirectly, a financial or other material benefit.

Cyber proxies—The use of intermediaries to contribute directly or indirectly to a cyber dependent crime intentionally targeting a state.

Cyberbullying—The use of information and communication technology by children to annoy, humiliate, insult, offend, harass, alarm, stalk, abuse or otherwise attack another child or children.

Cybercrime investigations—acts involving the discovery and preservation, and collection and securing of evidence to file and maintain a prosecution when a crime is deemed to have taken place in cyberspace.

Cybercrime taxonomy—the systematic classification and organization of entire areas regarding the knowledge, skills and approaches that must be commonly mastered in the implementation of cybercrime investigations.

Cybercrime—acts involving cyber space (including computers, computer software, computer networks, or embedded software controlling systems) that violate various strongly defined norms in society's collective consciousness.

Cyber-dependent crime—A cybercrime that would not be possible without the Internet and digital technologies.

Cyber-enabled crimes—A cybercrime facilitated by the Internet and digital technologies.

Cyberespionage—The use of information and communication technology by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country' s national security, economic competitiveness, and/or military strength.

Cyberharassment—The use of information and communication technology to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse an individual (or individuals).

Cybersecurity—The collection of strategies, frameworks, and measures that are designed to identify threats and vulnerabilities of systems, networks, services, and data to these threats; prevent the exploitation of vulnerabilities; mitigate the harm caused by materialized threats; and safeguard people, property, and information and communication technology.

Cybersecurity posture—A term used to describe the cybersecurity capabilities of a country, organization or business.

Cybersmearing—Posting or otherwise distributing of false information or rumours about an adult or child to damage the victim' s social standing, interpersonal relationships, and/or reputation.

Cyberspace—An environment accessed by Internet-enabled digital technology within which online activities take place.

Cyberstalking—The use of information and communication technology to commit a series of acts over a period of time designed to harass, annoy, attack, threaten, frighten, and/or verbally abuse an individual (or individuals).

Cyberterrorism—The cyber-dependent crimes perpetrated against critical infrastructure to cause some form of harm and to provoke fear in the target population.

Cyberwarfare—Cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack.

Dark Web—The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as darknet.

Darknet—The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialized software. Also known as Dark Web.

Data—Any form of representation of information that is processed by a system of a digital device. Also known as computer data or computer information.

Data hiding analysis—Type of analysis that searches for hidden data on a system.

Data mining—The retrieval of information from data sets.

Data modeling—the technique of organizing data (targeted items and events) on the basis of consistent rules.

Data preservation—Requests are made to service providers by law enforcement in an effort to retain data before it is deleted or altered in any way.

Data protection—The safeguarding of personal information and regulates its collection, storage, analysis, use, and sharing.

Data protection by design—Privacy measures embedded in the design of systems and technologies. Also known as privacy by design.

Data quality testing—putting the results of criminal investigation under scrutiny and measuring to assess their appropriateness.

Data warehouse—a large scale database for storing data extracted and rebuilt from multiple information sources that is used for information analysis and decision-making.

Deep Web—The part of the World Wide Web that is not indexed by search engines and is not easily accessible and/or available to the public.

Denial of service (DOS) attack—A cybercrime that interferes with systems by overwhelming servers with requests to prevent legitimate traffic from accessing a site and/or using a system.

Design patents—A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as industrial designs.

Deterrence—Discouraging illicit activity through punishment.

Digital evidence—Data obtained from information and communication technology. Also known as electronic evidence.

Digital footprint—Data left behind by ICT users that can reveal information about them, including age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history and concerns, psychological disorders, employment status, affiliations, relationships, geolocation, routines, and other activities.

Digital forensic process—The search, retrieval, preservation, and maintenance of digital evidence; description, explanation and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability and relevance to the case; and the reporting of evidence pertinent to the case.

Digital forensics—A branch of forensic science that applies matters of law to information and communication technology and digital evidence.

Digital piracy—The illegal download of a movie from a third-party website that does not have the right to distribute the copyrighted work.

Direct evidence—Evidence that establishes a fact.

Disinformation—The deliberate spreading of false information.

Disinhibition—The process whereby an individual demonstrates a lack of social restraint with regards to online behavior.

Dissociative anonymity—Individuals' detachment of their online behavior from their offline behavior due to the anonymity afforded to them when utilizing the Internet and digital technology.

Dissociative imagination—Individuals' view of cyberspace as a forum within which the rules of everyday interactions, codes of conduct, social norms, and/or laws do not apply, disinhibiting the individual to act in a manner contrary to offline rules of everyday interactions, codes of conduct, social norms, and/or laws.

Distributed Denial of Service (DDoS) attack—The use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers to prevent legitimate users' access.

Dogpiling—A tactic whereby users within an online space bombard victims with offensive, insulting, and threatening messages to silence the target, force them to take back what they said and/or apologize, or to force them to leave the platform.

Domain name—A pseudonymous representation of an IP address in an Internet (or web) browser.

Domain Name System (DNS)—Enables Internet access by translating domain names to IP address.

Doxing—Personal information about individuals posted online to cause the individual some form of harm.

Doxware—A form ransomware that perpetrators use against victims that releases the user' s data if ransom is not paid to decrypt the files and data.

Dual criminality—A clause in treaties requiring acts to be considered illegal in cooperating countries.

Electoral fraud—The use of unlawful tactics to influence elections.

Electronic Discovery (eDiscovery)—The process of searching, identifying, and preserving digital data for use as evidence in a legal proceeding.

Electronic evidence—Data obtained from information and communication technology. Also known as digital evidence.

Emergency management plan—Outlines instructions to be followed and actions to be taken in the event of a cybersecurity incident. Also known as business continuity plan.

Encryption—Measure that blocks third party access to users' information and communications by encoding data using a factorial method.

Event reconstruction—This process seeks to determine who was responsible for the event, what happened, where did the event occur, when did the event take place, and how the event unfolded, through the identification, collation, and linkage of data. Also known as crime reconstruction.

Expected utility theory—A theory that holds that people engage in actions when the expected utility from these actions is higher than the expected utility of engaging in other actions.

Fake news—Propaganda and disinformation masquerading as real news.

Fifth domain—A term used to describe cyberspace as another domain of warfare.

File carving—Search based on content identifiers.

Firewall—A security measure that restricts the free flow of information by blocking unauthorized network traffic data.

First responders—Individuals who respond first to the scene and are responsible for securing evidence at the scene.

Forensic relevance—The relevance of forensic data is determined by whether the digital evidence: links or rules out a connection between the perpetrator and the target and/or the crime scene; supports or refutes perpetrator, victim and/or witness testimony; identifies the perpetrator(s) of the cybercrime; provides investigate leads; provides information about the method of operation of the perpetrator; and shows that a crime has taken place.

Forensic—scientific tests or techniques used in the detection of crime.

Full vulnerability disclosure—Publicly publishing the software or hardware vulnerability through online forums and websites before a fix is available.

Functional analysis—The assessment of the performance and capabilities of systems and devices involved in events.

General deterrence—Punishment designed to send the message to others that similar illicit behavior will receive similar severe punishment.

Geographical indications—Symbols of products quality and the reputation of the place of its creation property, which cannot be used unless the product was developed in that region according to standards of practice. Also known as appellations of origin.

Gray-Hat hackers—hackers in the middle ground between White-Hat and Black-Hat hackers; computer experts who may hack into a system without the knowledge or consent of the owner but lack malicious or evil intent; they may report security issues that they find to a public forum as opposed to the site owner directly.

Hacking—Unauthorized access to systems, networks, and data.

Hard drive—An internal, persistent memory in a computer.

Hash—A calculated cryptographic value used to identify evidence.

Hearsay—Out of court statements.

Human flesh search engine—A term used to describe online users work together to identify a target and perpetrate coordinated online abuse against the target.

Identity management—The process of authenticating users' identities, identifying associated privileges, and granting user access based on these privileges.

Identity-related crime—A perpetrator unlawfully assumes and/or misappropriates the identity of the **victim and/or uses the i**dentity and/or information associated with the identity for illicit purposes.

Image-based sexual abuse—A form of sexual violence whereby sexually explicit images and/or **videos of the victims are inten**tionally created, distributed, or threatened to be distributed without the consent of the victims. This may be to cause some form of harm to the victim and/or to benefit the perpetrator in some way (e.g. monetary gain, sexual gratification, social status building and more).

Imaging—Creating a duplicate copy of the content of the digital device.

Impact analysis—consists of information about victims and the scope of cybercrime as indicated by the number of systems, users, etc. that were accessed or used without authorization.

Incident detection—The process of identifying threats by actively monitoring assets and finding anomalous activity.

Industrial control systems—Systems that command and control critical infrastructure processes.

Industrial designs—A form of intellectual property that includes designs that are created with the specific purpose of being aesthetically pleasing to consumers and impacts their choice between products. Also known as design patents.

Information warfare—The collection, distribution, modification, disruption, interference with, corruption, and degradation of information to gain some advantage over an adversary.

Inoculation theory—This theory holds that the way to inoculate individuals from persuasion attempts of others is to expose them to these attempts and given them tools they need to resist these attempts.

Insider Threat—employees, contractors, consultants, or partners who have access and use of internal information technology and services resources and exhibit inappropriate or malicious behaviors.

Integrity—Data is accurate and trustworthy and has not been modified.

Intellectual property (IP)—Products of creativity, such as works, innovations, creations, original expression of ideas, and secret business practices and processes, that individuals have rights to as prescribed by law.

Internet governance—The creation and application of Internet principles, rules, and procedures by various stakeholders to guide the use of the Internet and shape its development.

Internet of Things (IoT)—an evolving, rapidly expanding network of internet-enabled devices that can communicate with each other and function electronically in a variety of ways impacting daily life.

Internet penetration rate—The portion of the population in an area that uses the Internet.

Internet Protocol address (IP address)—A unique identifier assigned by an Internet service provider to an Internet-connected digital device to connect to the Internet.

Internet service provider (ISP)—Provides Internet services to a computer system or a system of another digital device.

Internet trolls—Individuals that purposely post rude, aggressive, and offensive remarks designed to create discord and discontent online.

Interpersonal cybercrime—Cybercrimes committed by individuals against other individuals with whom they are interacting, communicating, and/or having some form of real or imagined relationship.

Intrusion detection systems (IDS)—A cybersecurity measure that enables the detection of cyberattacks and unauthorized access and use of systems, networks, data, services, and related resources.

Jurisdiction—A state' s power and authority to enforce laws and punish non-compliance with laws.

Key performance indicators (KPIs)—Measures that are used to determine progress towards the realization of the strategic objectives of the national cybersecurity strategy.

Keyword searches—Search based on terms provided by the investigator.

Knowledge management—The process of identification and assessment of knowledge needs and the utilization of knowledge assets.

Letters rogatory—Written requests from national courts for evidence from a foreign country.

Logical extraction—The search for and acquisition of evidence from the file system location.

Malware—malicious software used to infect computer systems and automatically execute its routine; includes terms such as viruses, Trojans, worms, spyware, and ransomware.

Memory resident malware—unique malware that leaves no files on the hard disk to indicate it has been used to facilitate cybercrimes, making traditional detection and mitigation much more difficult.

Metadata—information about data; attributes of files and their relationship to users or operating system and storage/device configurations.

Microlaundering—A form of money-laundering whereby the perpetrators launder a significant amount of money through multiple small transactions.

Misinformation—False or inaccurate information.

Missing data—inconsistent data resulting from the value of a certain item in a certain case being missing.

Money mules—Individuals who either knowingly or unknowingly commit crimes and/or cybercrimes by obtaining and transferring illicit goods, engaging in illicit services, and/or illegally receiving or transferring money for others for remuneration.

Money-laundering—The concealment of illicit proceeds through a combination of legitimate and illegitimate transactions.

Morphing—A victim' s face or head superimposed on the bodies of others for the purpose of defamation, pornography, and/or sexual abuse.

Mutual legal assistance treaty (MLAT)—An agreement between countries to cooperate on investigations and prosecutions of certain and/or all offences proscribed by both parties under national law.

Net neutrality—Requires all data, irrespective of source, to be treated equally.

Neutralization techniques—Techniques used to overcome or minimize negative emotions associated with the engagement in illicit activity.

Non-content data—Data about the content. Also known as metadata.

Online child sexual abuse—The use of information and communication technology as a means to sexually abuse children.

Online child sexual exploitation—The use of information and communication technology as a means to sexually exploit children, where child sexual abuse and/or other sexualized acts using children involve an exchange of some kind.

Online impersonation—The impersonation of victims by creating accounts with similar names and, by making use of existing images of the victims.

Organized crime—A continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand.

Ownership and possession analysis—Type of analysis that is used to determine the person who created, accessed, and/or modified files on a computer system.

Passive digital footprint—Data that is obtained and unintentionally left behind by the users of the Internet and digital technology.

Patent—Exclusive right granted for an invention (innovation or creation), which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem.

Patent trolls—These individuals neither create nor invent anything; they merely purchase patents to license them to others, and sue any person, group, or organization infringing their acquired patents.

Pedophile—A person sexually interested in children.

Personal autonomy—The ability to make choices and act in ways of their own choosing free from coercion.

Pharming—The creation of a fake, duplicate website that is designed to trick users to input their login credentials.

Phishing—The sending of an email to targets with a website link for users to click on, which might either download malware onto the users' digital devices or sends users to a malicious website that is designed to steal users' credentials.

Physical extraction—The search for and acquisition of evidence from the location within a digital device where the evidence resides.

Preventive law—Legal rules that focus on regulation of risk and seek to prevent crime or at the very least mitigate the damage that could be caused in the event of a crime.

Privacy—The right to be left alone and be free from observation; the capacity to keep one's thoughts, beliefs, identity, and behavior secret; and the right to choose and control when, what, why, where, how, and to whom information about oneself is revealed and to what extent information is revealed.

Privacy by design—Privacy measures embedded in the design of systems and technologies. Also known as data protection by design.

Procedural law—Legal rules that cover the processes and procedures to be followed to apply substantive law, the rules to enable the enforcement of substantive law, and the rules and standards in criminal justice proceedings.

Proxy server—An intermediary server that is used to connect a client with a server that the client is requesting resources from.

Pseudonymization—The process whereby identifying data in a record is replaced by artificial identifiers.

Quality assurance and control—the process whereby, in relation to an analytical framework, an experienced and skilled person, by giving guidance and advice, can guarantee the quality of the final output.

Ransomware—Malware designed to take users' system, files, and/or data hostage and relinquish control back to the user only after ransom is paid.

Recovery—The identification, creation, and ultimate implementation of measures for resilience and the restoration of systems, networks, services, and data that were unavailable, harmed, damaged, and/or compromised during the incident.

Relational analysis—The determination of the individuals involved and what they did, and the association and relationships between these individuals.

Resilience—The ability to withstand disruptions, adapt to changing conditions, and recover from incidents of ICT and protect the confidentiality, integrity, and availability of systems, networks, services, and data.

Responsible vulnerability disclosure—The practice of not disclosing the vulnerability until a fix is provided by the responsible organization.

Revenge porn—when a revengeful partner publishes nonconsensual pornographic photos and videos on the Internet of their former partner.

Risk—The impact of a threat and its probability of occurring.

Risk assessment—The evaluation of the probability of a threat, its impact, and the exposure of an asset to this threat.

Risk treatment—Responses to risks.

Roasting—Individuals willingly posting images and/or videos of themselves on online and inviting others to post insults about them.

Rootkit—software that will modify the operating system of a victim computer and replace key functions with its own functionality in order to maintain a stealthy presence and remain undetected.

Routine activity theory—A theory that holds that crime occurs when two elements are present - a motivated offender and a suitable target, and one element is absent—a capable guardian.

Scope of cybercrime—the scale of cybercrime organizations as well as the scope of victims or their associated computers.

Script—A computer program.

Service provider—Provides services to a computer system or a system of another digital device.

Sexting—Self-generated sexually explicit material.

Sexting—sending sexually explicit photos of oneself to others.

Sextortion—A form of cyberharassment whereby the victim is threatened with the release of sexually explicit content if the demands of the perpetrator are not met.

Situational crime prevention—Measures used to prevent and reduce crime.

Smishing—Phishing via text messaging. Also known as SMS phishing.

SMS phishing—Phishing via text messaging. Also known as smishing.

Social dilemma—When individuals' decisions are based on self-interest rather than the interest of the group or collective, even when the utility of engaging in the collective interest is higher than the utility of engaging in self-interest.

Social engineering—A tactic whereby a perpetrator tricks the target into divulging information or performing another action.

Social engineering fraud—Tricking the victim into revealing or otherwise providing personal information and/or funds to the perpetrator.

Solipsistic introjection—The fictional image of others created by users' perceptions of others and their traits absent contextual data, including the relationships they have with them based on imagined rather than real information.

Sovereignty—A country's right to exercise authority over its own territory.

Spam—Sending of unsolicited emails.

Spearphishing—The sending of emails with infected attachments or links that are designed to dupe the receiver into clicking on the attachments or links.

Specific deterrence—Punishing individuals who commit crime to cease further illicit activity if the punishment received outweighs the benefits of committing the crime.

Spyware—Malware designed to surreptitiously monitor infected systems and collect and relay information back to creator and/or user of the spyware.

Stalkerware—A form of spyware that can run on a victim's computer, smartphone or other Internet-enabled digital device and collect and relay all the user's actions on these devices, from emails and text messages sent and received, to photographs taken and keystrokes.

Standard operating procedures—Documents that include the policies and sequential acts that should be followed to investigate cybercrime and handle digital evidence on information and communication technology.

Steganography—The stealthy concealment of data by both hiding content and making it invisible.

Substantive law—Legal rules that govern behaviour and responsibilities of those over whom the state has jurisdiction.

Surface Web—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Clearnet or Visible Web.

Swappers—Semiautomated cryptocurrency exchanges.

Temporal analysis—The determination of the time events occurred and the sequence of these events.

Territorial sovereignty—The state's complete and exclusive exercise of authority and power over its geographic territory.

Terrorism—threats or violent acts against people or property to affect government policy or political, religious, or ideological change.

Threat—A circumstance that could cause harm.

Threat actors—cyber criminals who give rise to threats to enterprises and organizations.

Threat profile—comprises a crime scenario, the threat actors, and information about the threat.

Time-frame analysis—Type of analysis that seeks to create a timeline or time sequence of actions using time stamps that led to an event or to determine the time and date a user performed some action.

Traceback—The process of tracing illicit acts back to the source of the cybercrime. Also known as back-tracing.

Trade secret theft—The theft of a trade secret offline and/or online to gain an unfair competitive advantage.

Trade secrets—Valuable information about business processes and practices that are secret and protect the business’ competitive advantage.

Trademark counterfeiting—Intentional unauthorized use of a trademark to label good or service that does not originate from the trademark owner.

Trademarks—Identifiers that distinguish the source of a good or service.

Traffic data—Data transmitted over a computer network (or network).

Trojan horse—Malware designed to look like legitimate software in order to trick the user into downloading the program, which infects the users’ system to spy, steal and/or cause harm.

Unallocated space—Space that is available for use because content was deleted, or space was never used.

Usability—Ease with which digital devices can be used.

Victimology—profile information related to the victim.

Virus—Malware that requires user activity to spread.

Vishing—Phishing via telecommunications.

Visible Web—Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Clearnet or Surface Web.

Vulnerability—Exposure to harm.

Watering-hole attack—Placing malware on the most frequented websites of targets to ultimately infect their systems and gain unauthorized access to them.

Web crawlers—Applications designed to traverse the World Wide Web to achieve specific objectives.

Whaling—Pretending to be higher level executives in a company, lawyers, accountants, and others in positions of authority and trust, in order to trick employees into sending them funds.

White-Hat (or ethical) hackers—hackers who break into systems to test their skills and to figure out how security programs work; professionals who have been authorized by an organization to compromise its network, report any security issues, and make recommendations on how to fix them.

Worm—Stand-alone malicious software that spreads without the need for user activity.

Write blocker—Designed to prevent the alteration of data during the copying process.

Zero day—Previously unknown vulnerability that is exploited once identified.

Bibliography

#mum cryptolabs. (2004, September 25). On the 2ROT13 Encryption Algorithm. Retrieved from http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf

114th U.S. Congress, Senate Bill 754, Cybersecurity Information Sharing Act of 2015. (2015, October 28). Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/754/text

ACCESSDATA Forensic Toolkit (FTK). (2016). Retrieved from http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

ACCESSDATA. (n.d.). Network investigation and incident response. Retrieved from http://accessdata.com/solutions/digital-forensics/ad-enterprise

AJMartel. (2016, April 21). IRTriage. GitHub. Retrieved from https://github.com/AJMartel/IRTriage

Akerlof, G. and Shiller, R. 2015. Phishing for phools. In Phishing for Phools. Princeton University Press.

Apache License 2.0. (n.d.). Retrieved from https://tldrlegal.com/license/apache-license-2.0-(apache-2.0)

Archambeault, William O. and Betty J. Archambeault. Computers in Criminal Justice Administration and Management: Introduction to Emerging Issues and Applications. Cincinnati: Anderson Publishing Co., 1984.

Arkin, Stanley, et al. Prevention and Prosecution of Computer and High Technology Crime. New York: Matthew Bender and Co., 1988.

Ashford, W. (2015, September 15). Most DDoS attacks hiding something more sinister, Neustar warns.

Associated Press. (1998, July 11). Man who threatened gates sentenced to prison - Extortion letter told

ATT&CK. 2015. MITRE ATT&CK. MITRE. Retrieved from https://attack.mitre.org/

Autopsy. (2016). Retrieved from http://www.sleuthkit.org/autopsy

Barta, C. (2011, December). NTDS.DIT forensics. Retrieved from http://ntdsxtract.com/downloads/ntdsxtract/ntds_forensics.pdf

Barufaldi, D. (n.d.). Hedge funds: Strategies. Investopedia. Retrieved from http://www.investopedia.com/university/hedge-fund/strategies.asp

Bash, K. (2015, May 5). PowerShell DSC for Linux is now available! [Blog post]. Retrieved from https://blogs.msdn.microsoft.com/powershell/2015/05/05/powershell-dsc-for-linux-is-now-available/

BatBlue. (n.d.). The Darknet – The underground for the underground. Retrieved from http://www.batblue.com/the-darknet/

Bequai, August. Computer Crime. Lexington, MA: Lexington Books, 1978.

Bequai, August. How to Prevent Computer Crime: A Guide For Managers. New York: John Wiley and Sons, 1983.

Bequai, August. Technocrimes. Lexington, MA: Lexington Books, 1987.

Bequai, August. Technocrimes-The Computerization of Crime and Terrorism. Lexington, MA: Lexington Books, 1986.

Bequai, August. "Technocrimes-Why the Cops Can't Cope." Law Enforcement Technology. March/April 1987: 28.

Bequai, August. White Collar Crime. Lexington, MA: Lexington Books, 1977.

Boyd, J. (n.d.). Summary of OODA model. Retrieved from http://www.valuebasedmanagement.net/methods_boyd_ooda_loop.html

Brezinski, D., Killalea, T. (2002, February). Guidelines for evidence collection and archiving. Retrieved from https://tools.ietf.org/html/rfc3227

BriMor Labs Tools. (2016). Retrieved from https://www.brimorlabs.com/tools/

British Standards Institution. (n.d.). Cyber security. Retrieved from http://www.bsigroup.com/en-GB/Cyber-Security/

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., and Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8(1), 1-20.

Bruneau, G. (2010). DNS Sinkhole. Retrieved from https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

Carman, A. (2015, October, 6). Study: Average cost of cybercrime rises again in 2015 to $7.7 million. SC Magazine. Retrieved from http://www.scmagazine.com/ponemon-and-hp-release-annual-cybercrime-cost-study/article/443433/

CBS News. (2016, January 8). Former St. Louis Cardinals executive pleads guilty to hacking Houston Astros. Retrieved from http://www.cbsnews.com/news/former-st-louis-cardinals-executive-pleads-guilty-to-hacking-houston-astros

Centers for Disease Control and Prevention. (2016). About Zika: What we know. Retrieved from http://www.cdc.gov/zika/about/

Cisco Snort. (n.d.). Retrieved from http://www.snort.org

Cleveland, T. (n.d.). SEC terminates cyber-fraud ring that netted $100 million in CFD trading. Forex Fraud. Retrieved from http://www.forexfraud.com/forex-articles/sec-terminates-cyber-fraud-ring-that-netted-$100-millionin-cfd-trading.html

Cluley, G. (2016, July 28). Citibank IT guy deliberately wiped routers, shut down 90% of firm' s networks across America. Tripwire. Retrieved from

http://www.tripwire.com/state-of-security/featured/citibank-it-guy-deliberately-wiped-routers-shutdown-90-of-firms-networks-across-america

clymb3r. (2015, September 30). PowerShell – Invoke-NinjaCopy. GitHub. Retrieved from https://github.com/clymb3r/PowerShell/tree/master/Invoke-NinjaCopy

Computer emergency response team. (n.d.). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Computer_emergency_response_team

Consumer Federation of America. (n.d.). Protect yourself from the "grandparent scam." Retrieved from http://www.consumerfed.org/pdfs/Grandparent-Scam-Tips.pdf

Cottim, A. (2010). Cybercrime, cyberterrorism and jurisdiction: An analysis of Article 22 of the COE Convention on Cybercrime. European Journal of Legal Studies. Retrieved from http://www.ejls.eu/6/78UK.htm

Council of Europe. (2016). Action against cybercrime. Retrieved from http://www.coe.int/cybercrime Council of Europe. (2016). Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

Council of Europe. (2016)., Details of Treaty No.185, Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

CounterTack Products. (2016). Retrieved from http://www.countertack.com/products

da667. (2015, November 2). Netstat. GitHub. Retrieved from https://github.com/da667/netstat/blob/master/netstat.py

Danyliw, R. Meijer, J., Demchenko, Y. (2007, December). The incident object description exchange format. Retrieved from https://tools.ietf.org/html/rfc5070

Das, K. N., Spicer, J. (2016, July 21). How the New York Fed fumbled over the Bangladesh Bank cyber-heist. Reuters Investigates. Retrieved from http://www.reuters.com/investigates/special-report/cyber-heist-federal/

David, W. and Pattavina, A. 2005. The Internet as a conduit for criminal activity. In Information technology and the criminal justice system. Sage.

Deacon, B. W. (2015, September 20). The Darknet (Deep Web) explained. LinkedIn Pulse. Retrieved from https://www.linkedin.com/pulse/darknet-deep-web-explained-bradley-w-deacon

D3FEND. 2022. D3FEND™, A knowledge graph of cybersecurity countermeasures. MITRE. Retrieved from https://d3fend.mitre.org/

Delhi_Cybercrime_Unit. 2022. Custom fraud via social networking sites. Special Cybercrime Unit, India. Retrieved from https://cyber.delhipolice. gov.in/socialmediacrimes.html

destijl. (2016, November 20). GRR rapid response: Remote live forensics for incident response. GitHub. Retrieved from https://github.com/google/grr

Dethlefs, R. (2015, May 1). How cyber attacks became more profitable than the drug trade. Fortune. Retrieved from http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/

Directive (EU) 2016/680 of the European Parliament and of the Council. (2016, April 27). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

Doyle, C. (2014, October 15). Cybercrime: A sketch of 18 U.S.C. 1030 and related federal criminal laws. Washington, DC: Congressional Research Service, Library of Congress. Retrieved from https://www.fas.org/sgp/crs/misc/RS20830.pdf

Ducklin, P. (2013, Jan 27). Not-so anonymous Anonymouses head off to prison over PayPal DDoS. Naked Security. Retrieved from https://nakedsecurity.sophos.com/2013/01/27/not-so-anonymous-anonymouses-head-off-to-prisonover-paypal-ddos/

elastic Products. (2016). Retrieved from https://www.elastic.co/products Electronic Privacy Information Center. (2016). Electronic Communications Privacy Act (ECPA). Retrieved from https://epic.org/privacy/ecpa/

Europol' s European Cybercrime Centre (EC3). (2015). Europol, Internet Organised Crime Threat Assessment (IOCTA) 2015. Retrieved from https://www.europol.europa.eu/iocta/2015/overview.html

Farivar, C. (2015, January 2). Come for lulz, stay for hacktivism: A new book on Anonymous, reviewed. Ars Technica. Retrieved from http://arstechnica.com/security/2015/01/come-for-the-lulz-stay-for-the-hacktivism-a-new-book-on-anonymous-reviewed/

Federal Bureau of Investigation. 2021. FBI Internet crime report 2021. Federal Bureau of Investigation. Retrieved from https://www.documentcloud.org/documents/21504639-fbi-internet-crime-report-2021

Federal Bureau of Investigation. (2010, October). Cyber theft ring [graphic]. Retrieved from https://archives.fbi.gov/archives/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-graphic

Federal Bureau of Investigation. (n.d.). Nigerian letter or “419” fraud. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud

Federal Bureau of Investigation. (n.d.). Uniform crime reporting. Retrieved from https://ucr.fbi.gov/

Federal Trade Commission. (2016, May 24). Marketers of “mosquito shield bands” to pay $300,000, barred from making misleading pest-control claims under settlement with FTC. Retrieved from https://www.ftc.gov/news-events/press-releases/2016/05/marketers-mosquito-shield-bands-pay-300000-barred-making

Federal Trade Commission. (n.d.). Cases tagged with data security. Retrieved from https://www.ftc.gov/enforcement/cases-proceedings/terms/249

Federal Trade Commission. (n.d.). Data security. Retrieved from https://www.ftc.gov/datasecurity

FEEBle Industries Forum. (n.d.). Retrieved from https://feeble-industries.com/forums/

Findings from Analysis of DNC intrusion malware. (2016, June 20). Retrieved from http://www.threatgeek.com/2016/06/dnc_update.html

Finkle, J. (2016, August 31). Exclusive: SWIFT discloses more cyberthefts, pressures banks on security. Reuters. Retrieved from http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C

Fitzpatrick, D., Griffin, D. (2016, April 4). “Ransomware” crime wave growing. CNNMoney. Retrieved from http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/

Flashpoint. (2016, June 2). Ransomware as a service: Inside an organized Russian ransomware campaign. Retrieved from https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf

ForensicsWiki – Hashing. (2009, May 5). Retrieved from http://www.forensicswiki.org/wiki/Hashing

Franceschi-Bicchierai, L. (2016, July 22). Ransomware gang claims Fortune 500 company hired them to hack the competition. Motherboard. Retrieved from
http://motherboard.vice.com/read/ransomware-gang-claims-fortune-500-company-hired-them-to-hack-the-competition

F-Response. (n.d.). Retrieved from https://www.f-response.com

Frizell, S. (2014, December 2). Sony executives' salaries leaked in devastating hack. Time. Retrieved from http://time.com/3615160/sony-hack-salaries/

F-Secure. (2016). Evaluation the customer journey of crypto-ransomware and the paradox behind it. Retrieved from https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf

F-Secure. (n.d.). Botnets. Retrieved from https://www.f-secure.com/en/web/labs_global/botnets

Ganson, M. (2015, July 20). .vbs script for computing and displaying md5 hashes. Retrieved from http://mwganson.freeyellow.com/md5/md5.vbs

Germano, J. H. (2014). CyberSecurity partnerships: A new era of public-private collaboration. New York, NY: The Center on Law and Security, New York University School of Law. Retrieved from http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf

gfoss. (2016, April 18). PSRecon. GitHub. Retrieved from https://github.com/gfoss/PSRecon/blob/master/psrecon.ps1

Goodman, M. (2015). Future crimes: Everything is connected, everyone is vulnerable and what we can do about it. Toronto, Ontario: Doubleday Canada.

Google hacking database (GHDB). (n.d.). Retrieved from https://www.exploit-db.com/google-hacking-database/

Greene, T. (2015, Sep 17). Under DDoS attack? Look for something worse. Network World. Retrieved from http://www.networkworld.com/article/2984648/security/under-ddos-attack-look-for-something-worse.html

Guidance Software EnCase Forensic. (n.d.). Retrieved from https://www.guidancesoftware.com/encase-forensic

Guidance Software. (n.d.). Retrieved from https://www.guidancesoftware.com/

Hacking tools: June 2013 [Blog post]. (2013, June) Retrieved from http://anonhacktivism.blogspot.com/2013/06/dos-tools-2.html

Handerhan, R. (2010). Japanese and American computer crime policy: A comparative study. Carnegie Mellon University Research Showcase. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1067&context=hsshonors

Harrell, C. (2013, September 12). Tools to grab locked files [Blog post]. Retrieved from http://journeyintoir.blogspot.com/2013/09/tools-to-grab-locked-files.html

Hern, A. (2016, August 3). Ransomware threat on the rise as "almost 40% of businesses attacked." The Guardian. Retrieved from https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

Holt, T. 2018. Regulating cybercrime through law enforcement and industry mechanisms. The ANNALS of the American Academy of Political and Social Science 679, 1 (2018).

Hutchins, E. M., Cloppert, M. J., Amin, R. M. (2014, April 3). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

IBM. 2022. X-Force Threat Intelligence Index 2022. International Business Machines Corporation (IBM). Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ

IC3. 2000. Internet Crime Complaint Center IC3. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/

IC4. 2022. National Cyber Crime Reporting Portal. Ministry of Home Affairs, India. Retrieved from https://cybercrime.gov.in/

InfraGard. (n.d.). Retrieved from https://www.infragard.org/

Internet Archive. (2014). Retrieved from https://archive.org/web/

Introduction to TAXII. (2012, November). Retrieved from https://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

ISACA. (2013). COBIT 5 for risk. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-5-Risk_res_Eng_1213.ppt

ISACA. (2016). What is COBIT 5? Retrieved from http://www.isaca.org/cobit/pages/default.aspx

IT Governance. (n.d.). Business continuity, disaster recovery and ISO22301. Retrieved from http://www.itgovernance.co.uk/bc_dr.aspx

IT Governance. (n.d.). Cyber security risk assessments (10 steps to cyber security). Retrieved from http://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security.aspx

IT Governance. (n.d.). ISO/IEC 20000: The international standard for service management. Retrieved from http://www.itgovernance.co.uk/iso20000.aspx

IT Governance. (n.d.). ITIL – IT Infrastructure Library for IT Service Management (ITSM) – ITIL 2011. Retrieved from http://www.itgovernance.co.uk/itil.aspx

Japan Computer Emergency Response Team Coordination Center [English version]. (2016). Retrieved from https://www.jpcert.or.jp/english/

Japan Cybercrime Control Center. (n.d.). Retrieved from https://www.jc3.or.jp/

Japan, Unauthorized Computer Access Law, Law No. 128 of 1999. (n.d.). Retrieved from http://www.cybercrimelaw.net/Japan.html

jaredcatkinson. (2016, November 15). PowerForensics. GitHub. Retrieved from https://github.com/Invoke-IR/PowerForensics

jdevaney. (2013, February 19). Viewing extended file properties via command line in Linux. Stack Exchange, Super User. Retrieved from http://superuser.com/questions/554291/viewing-extended-file-properties-via-command-line-in-linux

Josefsson, S. (2006, October). The Base16, Base32, and Base64 Data Encodings. Retrieved from https://tools.ietf.org/html/rfc4648

jschicht. (2016, June 27). RawCopy. GitHub. Retrieved from https://github.com/jschicht/RawCopy

Leyden, J. (2016, June 28). SWIFT hackers nick $10m from Ukraine bank. The Register. Retrieved from http://www.theregister.co.uk/2016/06/28/swift_victim_ukraine/

Loader, B. and Thomas, D. 2013. Cybercrime: Security and surveillance in the information age. Routledge.

Lockheed Martin. 2022. Cyber Kill Chain. Lockheed Martin Corporation. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Louis, C. (n.d.). Comparison of computer misuse acts around the world. Retrieved from http://www.rechtsanwalt-louis.de/european_computer_misuse_acts.htm

McGuire, M. 2019. It ain' t what it is, it' s the way that they do it? Why we still don' t understand cybercrime. In The human factor of cybercrime. Routledge.

McLeod, S. (2016). Maslow' s hierarchy of needs. Simply Psychology. Retrieved from http://www.simplypsychology.org/maslow.html

MEIT. 2016. Information Technology Act 2000. Goverment of India. Retrieved from https://www.meity.gov.in/content/information-technology act-2000

Mendelsohn, B. (1956). Une nouvelle branche de la science bio-psycho-sociale: La victimologie. Revue Internationale de Criminologie et de Police Technique, Vol.10, pp.95-109.

Menting, M. (2011). Cybercrime laws by country & other resources. Retrieved from http://www.academia.edu/1125166/Cybercrime_Laws_By_Country_and_Other_Resources_DOC

Microsoft Message Analyzer. (n.d.). Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=44226

Microsoft TechNet. (n.d.). Directory data store. Retrieved from https://technet.microsoft.com/en-us/library/cc961761.aspx

Microsoft. (n.d.). Crash dump analysis using the Windows debuggers (WinDbg). Retrieved from https://msdn.microsoft.com/en-us/library/windows/hardware/ff539316(v=vs.85).aspx

Microsoft. (n.d.). Microsoft Interflow. Retrieved from https://technet.microsoft.com/en-us/library/dn750892.aspx

Microsoft. (n.d.). NetStatisticsGet function. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/bb525390(v=vs.85).aspx

Microsoft. (n.d.). Network management functions. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/aa370675(v=vs.85).aspx

Microsoft. (n.d.). Process status API. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/ms684884(v=vs.85).aspx

MITRE Corporation. (2016). Cyber Observable eXpression (CybOX). Retrieved from http://cybox.mitre.org

MITRE Corporation. (2016). Structured Threat Information eXpression (STIX). Retrieved from https://stixproject.github.io/

MITRE Corporation. (2016). Trusted Automated eXchange of Indicator Information (TAXII). Retrieved from https://taxiiproject.github.io/

Moonsols (n.d.). Retrieved from http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

Murai, S. (2016, June 6). Ransomware making costly inroads into online Japan. The Japan Times. Retrieved from http://www.japantimes.co.jp/news/2016/06/06/reference/ransomware-making-costly-inroads-into-online-japan/#.V8mgEztrrww

National Council of ISACs. (2016). Retrieved from http://www.nationalisacs.org/member-isacs

National Council on Aging. (n.d.). Top 10 financial scams targeting seniors. Retrieved from https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/

National Cyber-Forensics & Training Alliance. (2016). Retrieved from https://www.ncfta.net/

National Institute of Standards and Technology, U.S. Department of Commerce. (2012, September). Guide for conducting risk assessments. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology, U.S. Department of Commerce. (2006, August). SP 800-86, Guide to integrating forensic techniques into incident response. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Natsui, T. (2003). Cybercrimes in Japan: Recent cases, legislations, problems and perspectives. NetSafe II Conference, Auckland, New Zealand. Retrieved from http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf

NEC. (n.d.). NEC' s superior internal systems are proof in themselves. Retrieved from http://www.nec.com/en/global/solutions/cybersecurity/efforts/index.html

Nelson, B., Phillips, A., Steuart, C. (2016). Guide to computer forensics and investigations (5th ed.). Retrieved from http://www.utc.edu/center-information-security-assurance/468--ch03.ppt

Network Associates. (1999). Introduction to Cryptography, Chapter 1. Retrieved from http://www.pgpi.org/doc/pgpintro/

Neustar. (2015). U.S. DDoS attacks and protection report, April 2015. Retrieved from https://www.neustar.biz/resources/whitepapers/ddos-attacks-protection-report-us-2015

Nmap. (n.d.). Retrieved from https://nmap.org/

Nurse, J. 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624 (2018).

Open Security Research. (n.d.). Retrieved from http://opensecurityresearch.com/files/FGET.zip

OpenIOC. (n.d.). Retrieved from http://www.openioc.org/

OWASP. (n.d.). Application threat modeling. Retrieved from https://www.owasp.org/index.php/Application_Threat_Modeling

OWASP. (n.d.). OWASP risk rating methodology. Retrieved from https://www.owasp.org/index.php/

OWASP_Risk_Rating_Methodology

Paganini, P. (2013, August 7). Cybercrime as a service. Infosec Institute. Retrieved from http://resources.infosecinstitute.com/cybercrime-as-a-service/

Parks, J. (2013). Fraudulent charities in the wake of disaster. Fraud Magazine. Retrieved from http://www.fraud-magazine.com/article.aspx?id=4294978232

Parker, Donn B. "Computer-Related White Collar Crime." In Geis, Gilbert, and Ezra Stotland, eds. White Collar Crime: Theory and Research. Beverly Hills: Sage, 1980.

PCI Security Standards Council. (2016). Retrieved from https://www.pcisecuritystandards.org/

Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., and Aiken, M., 2022. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences 2, 2 (2022).

Ponemon Institute, LLC. (2015). 2015 Cost of cybercrime study: United States [Blog post]. Retrieved from http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states

PowerShell Code Repository – Get-FileHash. (n.d.). Retrieved from http://poshcode.org/5815

proofpoint. 2022. Multi-Persona Impersonation. proofpoint. Retrieved from https://www.proofpoint.com/au/blog/threat-insight/ta453-uses-multipersona-impersonation-capitalize-fomo

Prox, B. (2014, December 18). Get-RegistryKeyLastWriteTime. Retrieved from https://gallery.technet.microsoft.com/scriptcenter/Get-RegistryKeyLastWriteTim-63f4dd96

Reeve, T. (2015, October 15). Japan facing explosion in cyber-crime, claims report. SC Magazine (U.K.). Retrieved from http://www.scmagazineuk.com/japan-facing-explosion-in-cyber-crime-claims-report/article/446174/

Rekall. (n.d.). Retrieved from http://www.rekall-forensic.com/

The Pmem Memory acquisition suite. (n.d.). Retrieved from http://www.rekall-forensic.com/docs/Tools/

Reuters. (2015, December 21). Trader pleads guilty in insider trading, hacking case. Fortune. Retrieved from http://fortune.com/2015/12/21/trader-pleads-guilty-in-insider-trading-hacking-case/

Reuters. (2016, April 4). The "Panama Papers" law firm responds to the massive data hack. Fortune. Retrieved from http://fortune.com/2016/04/04/panama-papers-law-firm/

Richet., JL., 2013. Laundering Money Online: a review of cybercriminals methods. arXiv preprint arXiv:1310.2368 (2013).

Riley, C. (2015, February 6). Insurance giant Anthem hit by massive data breach. CNN Tech. Retrieved from http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

Root cause analysis. (n.d.). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Root_cause_analysis

Royal Canadian Mounted Police. (2014). Cybercrime: an overview of incidents and issues in Canada - Defining cybercrime from a law enforcement perspective. Retrieved from http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec2

RT. (2013, October 2). FBI seizes "Silk Road" black market domain, arrests owner. Retrieved from https://www.rt.com/usa/silk-road-bitcoin-shut-650/

Russinovich, M. (2011, July 25). TCPView v3.05. Retrieved from https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx

Samani, R., Beek, C. (2015, November 20). A dummies guide to "insider trading" via botnet [Blog post]. Retrieved from https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet/

Samani, R., Beek, C. (2015, November 23). A dummies guide to “insider trading” via botnet, part 2 [Blog post]. Retrieved from https://blogs.mcafee.com/mcafee-labs/a-dummies-guide-to-insider-trading-via-botnet-part-2/

SANS Institute. (n.d.). FOR408: Windows Forensic Analysis [Course]. Retrieved from https://www.sans.org/course/windows-forensic-analysis

SANS Institute. (n.d.). FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting [Course]. Retrieved from https://www.sans.org/course/advanced-incident-response-threat-hunting-training

SANS Institute. (n.d.). FOR572: Advanced Network Forensics and Analysis [Course]. Retrieved from https://www.sans.org/course/advanced-network-forensics-analysis

Sarkar, H. 2022. Cybercrime Navigator. In collaboration with C3I Centre and Microsoft India. Retrieved from https://cybercrime.c3ihub.org/

SecureLogix. (2014, October 21). The surging threat of telephony denial of service attacks. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf

Shaw, S. (n.d.). A modern cybersecurity strategy: Building a budget. SAS Institute. Retrieved from http://www.sas.com/en_us/insights/articles/risk-fraud/a-modern-cybersecurity-strategy-building-a-budget.html

Shook, S. (n.d.). Green eggs & SPAM - Efficient incident response. Retrieved from https://info.cylance.com/incident-response-and-malware

Siddaway, R. (2011, June 29). IE history to CSV [Blog post]. Retrieved from https://richardspowershellblog.wordpress.com/2011/06/29/ie-history-to-csv/

Sidel, R. (2014, September 18). Home Depot’ s 56 million card breach bigger than Target’ s. The Wall Street Journal. Retrieved from http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

Sieber, Ulrich. The International Handbook on Computer Crime. New York: John Wiley and Sons, 1986.

Sloan, Irving J. The Computer and the Law. New York: Oceana Publications, 1984.

Somers, L. E. Economic Crimes-Investigative Principles and Techniques. 1984.

Splunk. (2016). Retrieved from http://www.splunk.com/

Standards New Zealand. (2016). Risk management. Retrieved from https://www.standards.govt.nz/search-and-buy-standards/standards-information/risk-managment/

Steptoe & Johnson LLP. (2016, January 21). Comparison of U.S. state and federal security break notification laws. Retrieved from http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf

SWIFT. (2016). Retrieved from https://www.swift.com/

Sylve, J. (2016, August 20). LiME. GitHub. Retrieved from http://code.google.com/p/lime-forensics/

Tabansky, L. (2012). Cybercrime: A national security issue? Military and Strategic Affairs, 4(3), 117-136.

Tang, R. (2015, October 4). Get-MemoryDump. Retrieved from https://gallery.technet.microsoft.com/scriptcenter/Get-MemoryDump-c5ab38d8

Tcpdump & Libpcap. (2016). Retrieved from http://www.tcpdump.org/

The Scripting Guys. (2014, January 15). Using PowerShell to Find Connected Network Adapters [Blog post]. Retrieved from https://blogs.technet.microsoft.com/heyscriptingguy/2014/01/15/using-powershell-to-find-connected-network-adapters/

The Tor Project. (n.d.). Retrieved from https://www.torproject.org/

The Volatility Foundation. (n.d.). Releases. Retrieved from http://www.volatilityfoundation.org/#!releases/component_71401

The White House, Office of the Press Secretary. (2015, February 13). Executive Order promoting private sector cybersecurity information sharing. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Title 18 U.S. Code, Section 1030 - Crimes and criminal procedure. (n.d.). Retrieved from https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-se c1030.pdf

Title 18 U.S. Code, Section 1030 - Fraud and related activity in connection with computers. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1030

Title 18 U.S. Code, Section 1341 - Frauds and swindles. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1341

Title 18 U.S. Code, Section 1343 - Fraud by wire, radio, or television. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1343

Title 28 U.S. Code of Federal Regulations, Section 0.85 - General functions. (n.d.) Retrieved from https://www.law.cornell.edu/cfr/text/28/0.85

Tittel, E., Lemons, M., Kyle, M. (n.d.). Introduction: Information security and cybersecurity certifications. TechTarget. Retrieved from http://searchsecurity.techtarget.com/tip/SearchSecuritycom-guide-to-information-security-certifications

Tittel, E., Lindros, K. (2016, November 7). Best computer forensics certifications for 2017. Tom's IT Pro. Retrieved from http://www.tomsitpro.com/articles/computer-forensics-certifications,2-650.html

Tixteco, M., Tixteco, L., Perez, G., Medina, L. (2016, May 22). Intrusion detection using indicators of compromise based on best practices and Windows event logs. ICIMP 2016: The Eleventh International Conference on Internet Monitoring and Protection. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=icimp_2016_2_20_30032

Trend Micro. (2015, August 31). A brief history of notable online banking trojans. Retrieved from http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

Trend Micro. (2016). Ransomware. Retrieved from http://www.trendmicro.com/vinfo/us/security/definition/ransomware

U.S. Computer Emergency Readiness Team. (n.d.). Information sharing specifications for cybersecurity. Retrieved from https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

U.S. Department of Homeland Security and Department of Justice. (2016, June 15). Guidance to assist non-federal entities to share cyber threat indicators and defensive measures with federal entities under the Cybersecurity Information Sharing Act of 2015. Retrieved from https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

U.S. Department of Homeland Security. (2016, June 21). Automated Indicator Sharing (AIS). Retrieved from https://www.dhs.gov/ais

U.S. Department of Homeland Security. (n.d.). U.S. Secret Service, electronic crimes task forces. Retrieved from https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20

Crimes%20Task%20Force.pdf

U.S. Department of Justice, Federal Bureau of Investigation. (2015). 2015 Internet crime report. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf

U.S. Department of Justice. (2012). Payment processor for scareware cybercrime ring sentenced to 48 months in prison. Retrieved from https://www.justice.gov/opa/pr/payment-processor-scareware-cybercrime-ring-sentenced-48-months-prison

U.S. Government Accountability Office. (2007). Cybercrime: Public and private entities face challenges in addressing cyber threats. Retrieved from http://www.gao.gov/products/GAO-07-705

U.S. Office of Personnel Management, Cybersecurity Resource Center. (2015). Cybersecurity incidents. Retrieved from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

U.S. Patriot Act. (2001, Jan 3). Retrieved from https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

U.S. Postal Inspection Service. (2008). A U.S. Postal Inspector' s Guide to Internet Safety for Children. Retrieved from http://docplayer.net/16377727-A-u-s-postal-inspector-s-guide-to-internet-safety-for-children.html

U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations. (2015, September 15). OCIE' s 2015 Cybersecurity Examination Initiative. Retrieved from https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

U.S. Securities and Exchange Commission. (2015, September 22). SEC charges investment advisor with failing to adopt proper cybersecurity policies and procedures prior to breach. Retrieved from https://www.sec.gov/news/pressrelease/2015-202.html

U.S. Securities and Exchange Commission. (2016, June 8). SEC: Morgan Stanley failed to safeguard customer data. Retrieved from https://www.sec.gov/news/pressrelease/2016-112.html

U.S. Securities and Exchange Commission. (2016, March 18). Regulation S-P. Retrieved from https://www.sec.gov/spotlight/regulation-s-p.htm

U.S. Securities and Exchange Commission. (2016, October 14). SEC Spotlight: Regulation SCI. Retrieved from https://www.sec.gov/spotlight/regulation-sci.shtml

United States Department of Justice, Offices of the United States Attorneys. (n.d.). Cyber crime. Retrieved from https://www.justice.gov/usao/priority-areas/cyber-crime

Urano, A. (2015). The Japanese underground: A TrendLabs research paper. Retrieved from http://www.trendmicro.nl/media/wp/wp-the-japanese-underground-en.pdf

US Legal Definitions. (n.d.). Cybercrimes law and legal definition. Retrieved from http://definitions.uslegal.com/c/cybercrimes/

Verizon. (2016). Verizon's 2016 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

VirusTotal. (n.d.). Retrieved from https://www.virustotal.com

Visgean. (2014, February 23). Zeus. GitHub. Retrieved from https://github.com/Visgean/Zeus

Vormetric Data Security. (2015). 2015 Vormetric insider threat report. Retrieved from https://www.vormetric.com/campaigns/insiderthreat/2015/pdf/insiderthreatreport-retail-0224.pdf

WGCL-TV/CBS 46. (2014, May 19). Police: International Nigerian crime ring operates from Atlanta suburbs. Retrieved from http://www.cbs46.com/story/25551165/police-international-nigerian-crime-ring-operates-out-of-atlanta-suburbs

What-when-how. (n.d.). Accreditation of forensic science laboratories. Retrieved from http://what-when-how.com/forensic-sciences/accreditation-of-forensic-science-laboratories/

WHOis.net. (2015). Retrieved from https://www.whois.net/

WikiLeaks. (n.d.). Retrieved from https://wikileaks.org/

Wilmot, F., Lindow, B. (2014). Threat intelligence: STIX and stones will break your foes. Splunk .conf2014. Retrieved from https://conf.splunk.com/session/2014/conf2014_FredWilmot_Splunk_Security.pdf

Windows Management Instrumentation Command (WMIC.exe). (n.d.). Retrieved from http://ss64.com/nt/wmic.html

Windows Sysinternals. (2016). Retrieved from https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

WinPcap. (n.d.). Retrieved from https://www.winpcap.org/

Wireshark. (n.d.). Retrieved from https://www.wireshark.org/

X-Ways Forensics: Integrated Computer Forensics Software (n.d.). Retrieved from http://www.x-ways.net/forensics/index-m.html

YARA Project. (n.d.). Retrieved from https://code.google.com/p/yara-project

Index of Key Terms

[Production cooperation]
Editing: Kenji Shinoda
Design: Estem (Hiroyoshi Taniguchi, Tamotsu Yokono)

Afterword

We' re honored to be part of this second edition of the Cybercrime Investigation Body of Knowledge (CIBOK) and thank the authors, reviewers, and contributors whose exceptional effort, expertise, and insight brought it to life. The depth and breadth of this publication reflect the evolving challenges—and critical responsibilities—we all share in the field of cybercrime investigation. Its contributors, seasoned professionals from around the world, have combined deep technical and investigative experience with a spirit of global collaboration that' s essential for confronting today' s sophisticated and borderless threats.

●The Convergence of Physical Security and Cyber Threats

As technology leaders at one of the world' s preeminent security companies, we' ve had the unique vantage point of seeing the convergence of the physical and cyber threat landscapes begin to unfold. Our organization helps protect critical infrastructure, financial institutions, global logistics networks, and public venues—domains where the distinction between a physical breach and a cyber breach is diminishing. Physical and cyber threats now feed each other—what starts in one domain can quickly escalate into the other. The line between cybercrime and physical crime is blurring, and one day may disappear entirely. It' s important to recognize that we all now operate at the intersection of physical and digital risk—and that requires our teams and technology to be both physical- and cyber-aware by design.

●The Reality of Crime

The reality is clear: a crime is a crime, whether perpetrated with a crowbar or a keyboard. Whether an organization is breached through a back door or through a compromised credential, the intent, impact, and urgency are the same. In both worlds, the principles of safety, prevention, investigation, attribution, and resolution should be applied with the same rigor, the same sense of justice, and the same determination to help protect people, assets, and communities.

Translating cyber threats into investigations requires more than just forensic tools or detection technologies. It demands a mindset shift—a recognition that digital evidence carries weight, that behavior should be scrutinized without bias, and that cyber actors, like their physical counterparts, leave behind patterns and trails that reveal intent.

●Insider Threats

Insider threats often exploit both physical and cyber weaknesses. A rogue employee or trusted third party may use authorized access to bypass firewalls just as they might swipe a badge to enter restricted spaces. The investigation should treat both actions as part of a single threat vector, not as isolated events in separate domains. The holistic approach championed in the CIBOK—grounded in taxonomy, evidence handling, and investigative frameworks—aligns with the kind of multidisciplinary response today' s environment demands.

●Foundational Material for the Next Generation

This guide offers a helpful blueprint not only for investigators, but also for technology leaders, business executives, and security professionals who design, implement, and oversee security programs that are resilient, intelligent, and integrated. As technology leaders, we' re not just technologists—we' re stewards of trust. And when that trust is broken—through fraud, theft, sabotage, or negligence—we have an obligation to respond. Our responsibility is to understand the nature and impact of compromise to our business and colleagues and respond appropriately. CIBOK helps us do that with discipline and purpose.

This guide serves as a foundational resource for the next generation of investigators and leaders who will help shape the future of cyber defense and criminal justice. As physical and digital domains continue to merge, we should strive to evolve our response—and continue to insist on accountability, wherever and however crime is committed.

Mark Mullison
Chief Technology Officer
Allied Universal

Deanna Steele
Chief Information Officer – North America
Allied Universal