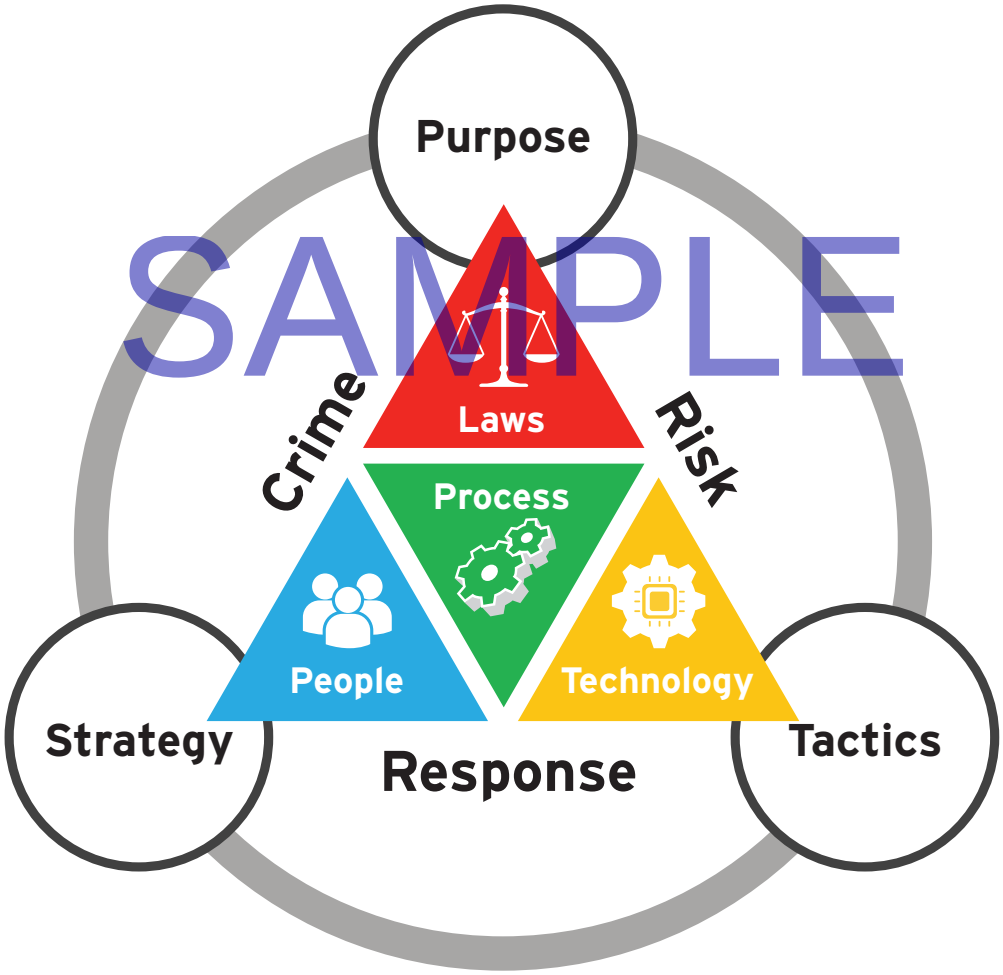
Cybercrime Investigation Body Of Knowledge

1st Edition

SAMPLE

A Guide to the

Cybercrime Investigation Body of Knowledge



All statements of fact, opinion, or analysis expressed are the authors' alone and do not necessarily reflect the official positions or views of the Department of Justice (DOJ) or any other U.S. government agency. Relevant chapters have been reviewed by DOJ to prevent the disclosure of classified or otherwise sensitive information.

The Publisher;
CIBOK Editorial Committee

Sponsored by Trend Micro, Incorporated.

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

Judith H. Germano is the founding member of Germano Law LLC, a law firm specializing in advising companies on cybersecurity governance and data privacy issues. Ms. Germano is an Adjunct Professor at New York University (NYU) School of Law and a Senior Fellow at the New York University 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.*

Craig W. Sorum is a 25-year 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).

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.

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.

Eric Zimmerman is a senior director 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.

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.

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.

John Jolly is the Vice President of Customer Success at Syncurity. Prior to joining Syncurity John was 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.

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.

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).

Reviewers

A special thanks to the following individuals who reviewed the draft edition of the CIBOK. Each provided important feedback to assist the authors. The list of contributors and reviewers will expand over time as this CIBOK evolves.

Reviewers

Richard Nolan, Global Managing Director of Cyber Investigations, Citi
Nicholas Peach, Senior Vice President, Information Security Executive, Bank of America/Merrill Lynch
Ronald Ritchey, Managing Director, JPMorgan Chase & Co.
Michael Woodson, VP, State Street
G. Bobby Singh, CISO, TMX Group
Avner Ziv, CIO, Bank of Israel
John R. Riley, Division Chief (Cyber Division), US Department of Homeland Security
Goran Oparnica, Managing Director, INsig2
Benoit Piton, CISO, BNP Paribas France
Dr. Richard Schroth, Executive Director and Executive in Residence, the Kogod Cybersecurity Governance Center at American University
John Walton, Azure Security, Microsoft Corporation
Carmen Oveissi-Fields, Partner/Global CISO, Deloitte
Ron Gula, Founder Tenable Network Security
Michael J. Hershman, CEO, Fairfax Group / ICSS

CIBOK Organizing Committee

The CIBOK was conceived and organized by the following individuals who contributed their talents and efforts to produce this important work.

Executive Editor and Principal Author, Shane Shook
Executive Producer, Trend Micro Corporate Officer of Japan Region, Satoshi Shimizu
Executive Director, Proseed Corporation CEO, Hiroshi Nishino
Senior Coordinator, Trend Micro Incorporated Director, Masakazu Yasumoto
Contributing Author and Project Member, Trend Micro Incorporated Senior Researcher, Noriaki Hayashi
Style Editor and Project Controller, Trend Micro Incorporated Senior Specialist, Yuka Miyatake
Project Consultant, Proseed Corporation Senior Consultant, Tetsuri Sawada

CIBOK Table of Contents

Introduction

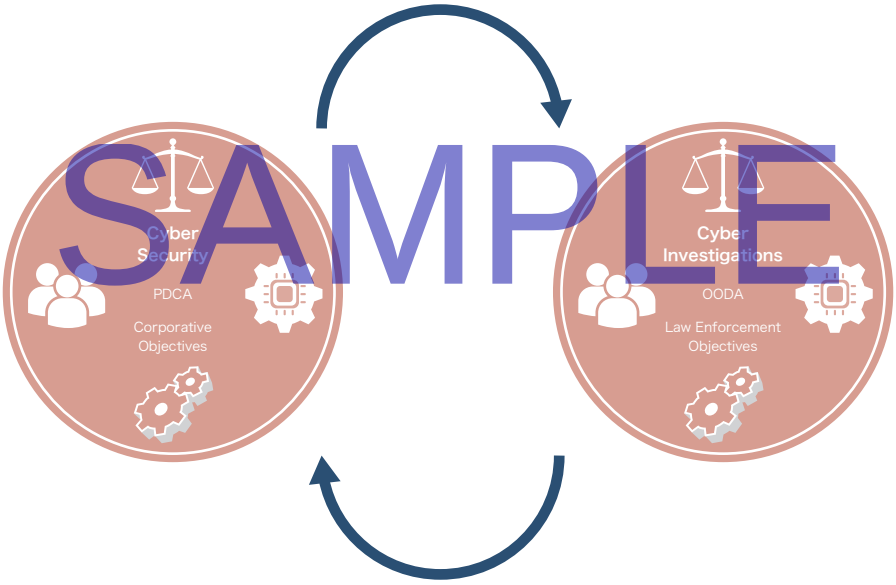
Introduction to the Guide

SAMPLE

Target Readers

The following groups and individuals are considered to be the target readers of this document.

- Police organizations or law enforcement agencies (prosecutors, courts) conducting criminal investigations, staff members of organizations conducting similar professional duties (organizations with recognized police powers such as the right to investigate, the right to arrest, etc.), staff members investigating organizational misdeeds, persons who have experience relating to criminal investigations but who do not know what to do when confronted with the term "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 are expected to be appointed as persons responsible for cybercrime investigation divisions in the future
- Persons who conduct research/development/instruction in programs which train cybercrime investigators and can exhibit a high level of effectiveness in a short period of time



Same coin, different focus

The Concept of "CIBOK"

What is the Reason for CIBOK?

Cyber security is a function of Information Technology (IT) to identify and mitigate risks to the organization. The organization has operating risks and related control 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 continuity of the organization's ability to serve customers (downstream) and to satisfy executive management in their obligations to satisfy the market, shareholders, and partners.

As IT has evolved to support organizational requirements, related evolution in methods to leverage technology as a tool, to target IT used by a company, or to disrupt or distract organizational functions through cyber means has coincidentally occurred. The Chief Information Officer (CIO) is a role that has gained a "seat at the boardroom table" for organizational strategy, and part of their role is to ensure the continuity of operations through IT support – including information protection and infrastructure security. To support that role, the Chief Information Security Officer (CISO) has been created for strategic and tactical planning and management of necessary resources. The rapid advance of IT and correlated threats, however, has created requirements that particular skills, knowledge and experience are needed to satisfy. Corresponding to those threats and related requirements, market intelligence (open source and proprietary) has evolved that creates new risks to the organization. In order to support the coincidental investigative and intelligence needs of the organization, the Cybercrime Investigator role has emerged. CIBOK is intended to describe the needs, background, and requirements to assist law enforcement and corporate risk managers, including IT.

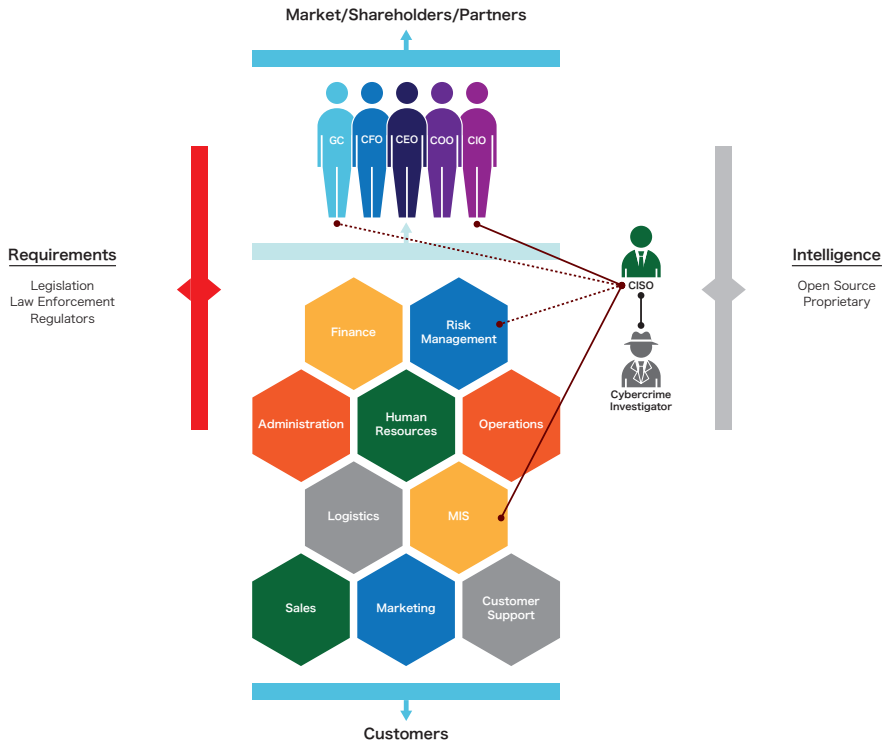


Figure 1. Cybercrime Investigation Function

The Objective of "CIBOK"

What is the Objective of this Document?

The objective of "**Cybercrime Investigation Body of Knowledge: CIBOK**" lies in demonstrating the "**good practice**" that capable and skillful cybercrime investigators implement in their investigation activities.

This purpose is to demonstrate "**taxonomy**" - the systematic classification and organization of entire areas regarding the knowledge, skills and approaches that must be commonly mastered in the implementation of investigations of cybercrime - and thereby provide means of access to use the topics included within. 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 material.

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 concerning consistent cybercrime investigations throughout the entire world, not dependent on the laws of each country.
2. Detailed demonstration of the positioning of other systematized customary practices, project management, computer science and digital forensics within the scope of cybercrime investigations.
3. Characterizing and demonstrating the content that should be put into practice in cybercrime investigations.
4. Presenting means to utilize the topics concerning the body of knowledge of cybercrime investigations.
5. To provide the basis necessary to prove that training curricula development and individual knowledge and skills pertaining to duties are of a high level.

In order to achieve these objectives, the following activities are being carried out.

In order to achieve the first objective (knowledge concerning consistent worldwide cybercrime investigations), this document has been created with the participation of 12 authors from 3 countries, including reviews in its development process.

In order to achieve the second objective (detailed demonstration of positioning within the scope of other systematized customary practices and cybercrime investigations), certain materials have been deemed essential to include in cybercrime investigations 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 2).

Chapter 1

Cybercrime and its Investigation

Introduction

Crimes have always been a factor in society. Crimes are committed by humans for varied reasons, or 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 by using 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.

This chapter will explore the legal principles that relate to cybercrimes, how they 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 for an applicable framework.

Learning this knowledge domain will allow readers to acquire an understanding of the following.

- What do the courts and laws define as "cybercrime"?
- What jurisdictions govern cybercrime investigations?
- What are "best practices" for cybercrime investigations?

Chapter 2

Types of Cybercrimes

Introduction

Social outcry and demonstrations against injustices ascribed to businesses used to be the domain of organized groups with picket signs in front of a business. Today such social outcry is performed with social media, or by defacing business marketing information such as websites. An associated 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 that is achieved through denial of service attacks or sabotage through tools 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 that is facilitated by ransomware. Espionage (commercial or government) has always existed but is today facilitated by backdoor Trojans that enable remote access and eavesdropping.

What are the "types" of crime that cyber 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. Associated descriptions of such objectives and their supporting motivations, profiles of actors and victims, and identifying characteristics of cybercriminals will also be provided.

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.

Learning this knowledge domain will allow readers to acquire an understanding of the following.

- What is "cybercrime"?
- What are the objectives and motivations?
- What are the profiles of cyber-criminals?
- How are cyber-criminals organized?
- What skills and knowledge to cyber-criminals have?
- How has cybercrime evolved?

Chapter 3

Artifacts of Cybercrimes

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 (TTPs) 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 "artifacts".

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?

Chapter 4

Scope of Cybercrimes

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 area 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 (TTPs). 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.

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 TTPs 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 do risks to those functions differ in public versus private organizations?

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, or are distributed actions (either for-hire or by organized criminal groups), or are repeated in different forms – revealing such 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.

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?

Chapter 6

Methods of Evidence Collection

Introduction

How an investigator collects evidence from source is as or even sometimes more important than the crime that a suspect is charged with. Many examples are available of prosecutions that have failed due to improper evidence collection or handling; similarly, there are many examples of associated criminal charges being sought based upon previously collected evidence. The nature, scope, and TTP's of cybercrimes will determine what types of evidence (and from which sources) are available.

This chapter will examine automated and manual methods of evidence collection according to the nature, scope, and TTP's of the relative types of cybercrime. Specific differences related to requirements by type of cybercrime will be reviewed as a cybercrime may relate later to other crimes, or may have jurisdictional requirements according to the scope and impact of the crime. Crimes against humans differ from business interruption or intellectual property theft, for example; thus such differences will be explored.

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.

This chapter includes methods of evidence collection from computers for analysis to be performed by qualified investigators. Several methods and tools are described, but it is not an "incident response" guide. The focus of the chapter is to assist with the collection of artifacts from sources of evidence previously discussed. The topics of cyber security and cybercrime investigations are related but this chapter should help readers understand a practical difference between IT activities and investigations – evidence collection.

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

- 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?

Chapter 7

Methods of Evidence Analysis

Introduction

In the "Methods of Evidence Analysis" knowledge domain, cybercrime investigators never treat evidence as coincidence – evidence is aggregated and analyzed through specific examination methods.

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 dissociate and consider cybercrime by scope, stage, and type in order to identify risks and threats related to the organization. It also includes profiles of, for example, "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 to define "policies," "systems," and "procedures" related to prevention and protection.

This knowledge domain is divided into three topics, which are closely related to "Sources of Evidence" (Chapter 5) and "Methods of Evidence Collection" (Chapter 6).

Just as the collection of appropriate evidence from the available sources is important for cybercrime investigators, evidence analysis is important for evaluating the scope of the cybercrime.

In general, investigations have constraints. Therefore, technology and other resources should be allocated in accordance with the evaluated scope.
At this time, efficiency and effectiveness in evidence analysis become the difference between carrying out appropriate cybercrime investigations and future enemies to prevent, or the difference between suffering from similar (or worsening) cybercrime and the preparation of future-oriented cybercrime prevention equipment.

The points above illustrate that this knowledge domain is related to all other aspects in cybercrime investigations, and is linked to all other 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?

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 which 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.

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 the incident according to organizational or jurisdictional policies. Because different cybercrimes differ in their impact, so too will they require different investigative and resolution techniques.

This chapter will 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 one 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 methods of communication, 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?

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) or inadvertently (an IP address that was logged by a sensor, a malware binary). When law enforcement or other investigators initially respond to the crime the initial information that is available 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 that may be useful for attribution (identification of the individual or group behind the crime) or for understanding or ascribing motive.

That evidence can be helpful to investigators to build experience for future cases and efficiencies for analysis and prosecution; however, that evidence represents artifacts only the specific victim as a source. Because of today's "sharing" economy of knowledge, skills, 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 for this primary 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 must necessarily limit the types of information that can be shared due to sensitivities of privacy or investigatory details that are crucial to 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 to interrupting cybercrimes.

This chapter will describe the methods and associated limitations of information sharing about cybercrimes. In particular it will illustrate the jurisdictional and classification limitations by types of crime, and the authorities for release and sharing of related information. Guidance will also be provided concerning documentation and qualification of information to be shared, as well as the timeliness and purposes of sharing. This chapter will provide investigators with a reference framework for sharing information 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:

- Why should cybercrime information be shared?
- Who should share cybercrime information – internally and externally?
- What requirements govern which type of information to share, and when?
- In what venues and how should cybercrime information be shared?

Chapter 10

Management Framework

Introduction

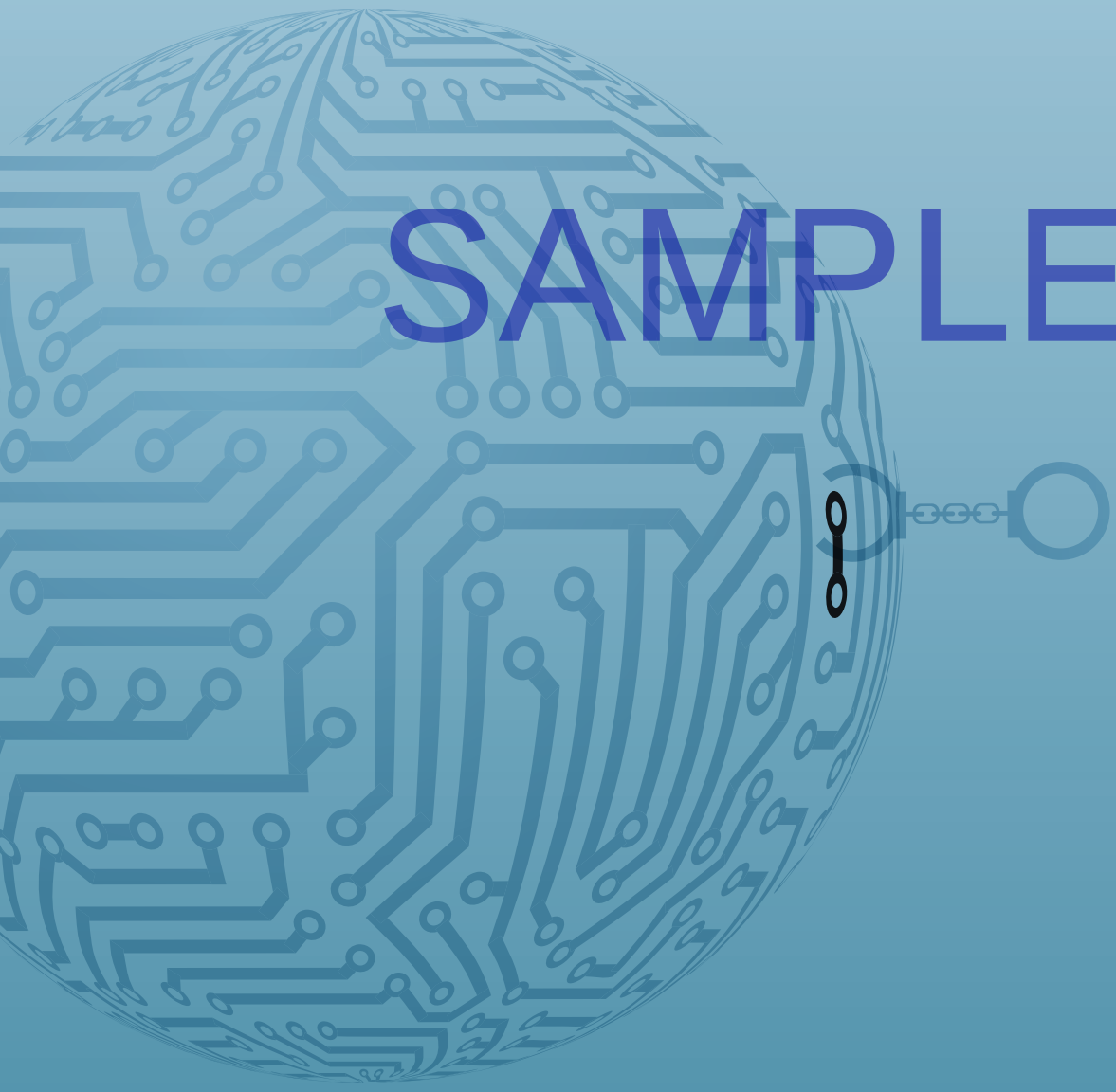
Every organization, whether public or private, has limited resources to support functions and related procedures. Those resources must be managed for efficiency of scale and scope of application. Incident response, investigation, and resolution of cybercrimes is a relatively new activity for organizations that has not heretofore been organized as a common function (as compared to finance, administration, information services, or customer support).

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 procedures and tools - crimes committed with cyber tools or facilitated by cyber TTP's are a new dimension for organizations to investigate and defend against, and define associated procedures and tools. Descriptions of hierarchical and matrixed organizational structures will be associated to the activities performed by the cyber investigations function and personnel.

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 purpose of a cybercrime investigation and resolution function?
- How should the function be organized and managed?
- What is the strategic objective of that function?
- What are resource requirements (staff, tools, and community) of the function?
- What are the technical and experiential requirements to staff, manage, and lead/govern that function?
- How should the function's (and related staff) performance be measured?
- What organizational communications and strategic involvement, in which organizational channels, should be implemented for success?
- Which organizational executive function(s) should the cybercrime investigations and resolution function report to?


SAMPLE