Professional Training Course

- Cybercrime Investigation Body of Knowledge -

(First Edition©)

Overview

The expanded use of the Internet has facilitated rapid advances in communications, systems control, and information sharing. Those advances have created enormous opportunities for society, commerce and trade to grow and adapt to near-real time access to each to information services.

Related to that growth, however, has been the intrusion of criminal actors who take advantage of the same services to commit traditional types of crimes in innovative ways that exceed by many magnitudes previous scales of theft, fraud, intimidation, and extortion. What began as disassociated efforts of individuals seeking attention or personal gain, has since become organized and syndicated activities.

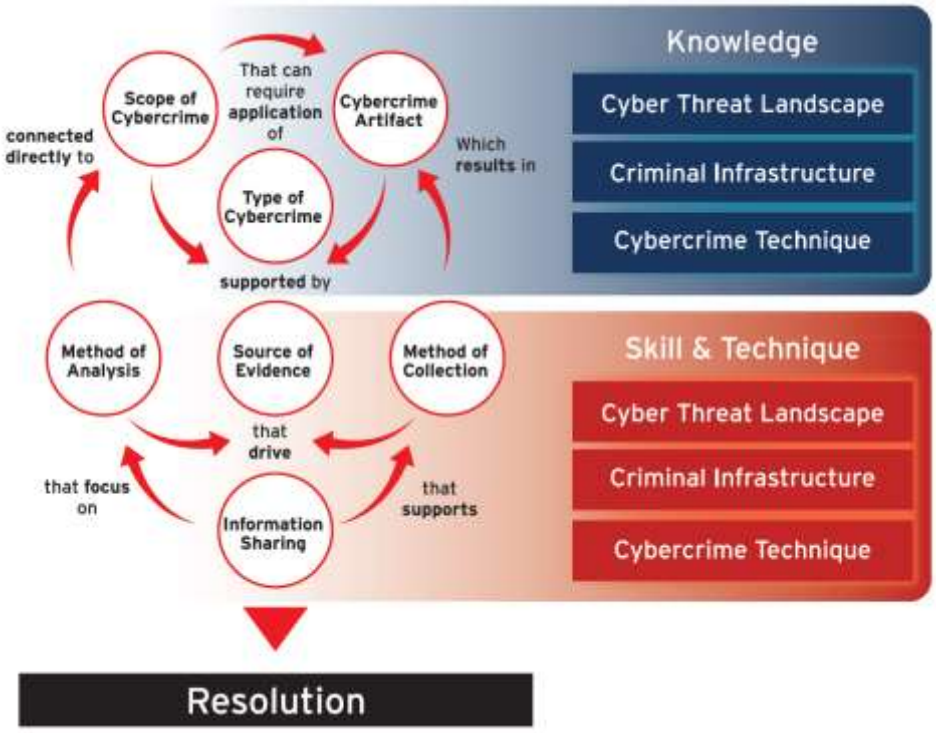
Those criminal activities offer speed and (some) anonymity with techniques that are difficult to keep pace with in traditional investigative methods. To address these challenges, law enforcement investigators and prosecutors, and corporate incident responders and risk management executives collaborated to create the Cyber Investigation Body of Knowledge – as a standard of practice to align law enforcement and corporate understanding and approaches in investigation and response.

For more details, please contact: secretariat@cibok.org

Objectives.

An overview of the knowledge, skills and techniques required by law enforcement and corporate security officers (and executives) to understand how to identify, respond, and investigate cybercrimes will be covered including:

1. Popularizing and promoting a commonsense approach concerning consistent international cybercrime investigations, not dependent upon the laws of each country.
2. Offering a 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 covered in this body of knowledge of cybercrime investigations collected from experienced professionals.
5. To provide a framework for developing training curricula and individual knowledge and skills pertaining to duties of investigators and responders.



For more details, please contact: secretariat@cibok.org

Topics

This 5-day course will provide a description with supporting interactive exercises concerning the following topics:

- Introduction to CIBOK
- Cybercrime and its Investigation
- Types of Cybercrimes
- Artifacts of Cybercrime
- Scope of Cybercrime
- Sources of Evidence
- Methods of Evidence Collection
- Methods of Evidence Analysis
- Incident Resolution
- Cybercrime Information Sharing
- Management Framework

Who should take this course

This course is designed as an executive introduction for law enforcement investigators and prosecutors, and corporate auditors and incident handlers who may be tasked with related risk and compliance assessments and mitigation.

What participants will be provided

Participants will be provided with a copy of the CIBOK First Edition©, a course manual, and reference materials.

Trainers

Dr. Shane Shook is a well-known veteran of information security and response engagements with nearly 30 years of experience spanning government and industry issues. He has led forensic analysts and provided expert testimony in many of the most notorious breaches involving financial services, healthcare, retail, hospitality, transportation, energy, automotive, and entertainment corporate (and government) systems. He has also served as expert witness in related federal, civil and commercial disputes. He currently serves on the advisory boards of several emerging security technology companies.

Topic	Objective
Day 1-2: Knowledge Development • The 5 objectives of CIBOK • What is a Cybercrime? - Technology as a Target - Technology as a Tool - Technology as a Distraction • What are Cybercrime Investigations? - With evidence of data/other loss - Without evidence of loss • What are challenges to Cybercrime Investigations? - Jurisdiction and Venue - Human Rights and Privacy • What skills, knowledge and experience are necessary to develop investigative capabilities to address Cybercrime?	To understand, through examples, the types, scope, artifacts of, and approaches to identifying and investigating Cybercrimes. To include jurisdictional considerations and information sharing within international privacy boundaries. *Case Examples*: - Retail/POS Breaches - Tech/Defense IP Theft - Healthcare/Gov Data Theft - Bank ATM/Payments Network Theft - Securities Fraud - Social Networks/Services Identity Theft and Fraud

The knowledge development, while generally intended to assist organizational stakeholders in understanding the types of Cybercrime (by objective), is an important foundation for investigators and analysts to become aware of the scope of Cybercrimes and the types of communication and decision-making that executive leaders must make.

It is recommended that *executive stakeholders*, as well as *lead investigators* or *department managers* participate in this section of training. It is also recommended that investigators and analysts attend this section to gain understanding of how their tasks are associated to strategic prevention, detection, and investigation of Cybercrimes.

The knowledge development section will conclude with a table-top exercise depicting a real-world cybercrime.

For more details, please contact: secretariat@cibok.org

Topic	Objective
Day 3-5: Skills Development • What is "evidence" vs. "artifacts" of cybercrime? • What are the sources of evidence? • What are the methods of evidence collection? • How should evidence be handled for investigative and judicial purposes? • What are methods of analysis for evidence of Cybercrimes? • What sources of information are available to intelligently discover or prevent Cybercrimes? • How should information about Cybercrimes be shared? • What are the minimum organizational requirements for a Cybercrimes investigation unit? • What tools and training are available to develop Cybercrimes investigation staff?	To understand the practical requirements for conducting a Cybercrime investigation. To include the identification (and discretion) of crimes versus anomalous activities, and methods of evidence collection and handling – for analysis. Also to include methods of efficient collection, processing and analysis with popular expert tools. Technical demonstrations, with associated exercises (and samples), will be performed for discussion.
The skills development is intended to expose participants to sources of evidence for consideration when conducting a cybercrime investigation. Such sources include external threat intelligence, industry and law enforcement intelligence, internet proprietary and open source information, and (some) discussion of dark/deep web. Additional sources will include security research *samples and evidence from network, file and operating systems, and live memory acquisition*. Methods of collection, processing and analysis will be covered with particular emphasis on appropriate documentation, custodial control and documentation of such evidence. It is recommended that technical and non-technical investigators and department managers participate in this section of training to understand skills and knowledge requirements of cybercrimes investigation functions and staffing. The skills development section will include technical analysis exercises.	