Cybersecurity Digital Forensics

Cyberincidents are fast moving and increasing in number and severity. When a cyberincident occurs, the attacked enterprise responds with a set of predetermined actions. Applying digital forensics to aid in the recovery and investigation of material on digital media and networks is one of these actions. Digital forensics is the “process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law).” The purpose of this white paper is to provide an overview of digital forensics as it applies to cybersecurity.
Cybersecurity Digital Forensics

Cyberincidents are fast moving and increasing in number and severity. When a cyberincident occurs, the attacked enterprise responds with a set of predetermined actions. Applying digital forensics to aid in the recovery and investigation of material on digital media and networks is one of these actions. Digital forensics is the “process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law).”¹ The purpose of this white paper is to provide an overview of digital forensics as it applies to cybersecurity.

The methods that digital forensics uses to handle digital evidence are very much grounded in the field’s roots in the scientific method of forensic science. Every forensic science certification requires a code of conduct of an unbiased and ethical approach to examinations.

BRIEF HISTORY OF DIGITAL FORENSICS
Digital forensics is nearly 40 years old, beginning in the late 1970s as a response to a demand for service from the law enforcement community (see figure 1). Most of the first criminal cases that involved computers were for financial fraud.² In the 1980s, digital forensics training courses were developed by organizations such as the Association of Certified Fraud Examiners, the National Consortium for Justice Information and Statistics, and the High Technology Crime Investigation Association (HTCIA); the first digital forensics company, Access Data, was formed; and the International Association of Computer Investigative Specialists (IACIS) was formed.³ Today, students can earn a Bachelor of Science degree in Computer Forensics and Digital Investigations.

1 Mohay, George M.; Alison Anderson; Byron Collie; Rodney D. McKemmish; Olivier de Vel; Computer and Intrusion Forensics, Artech House, USA, 2003
2 Ibid.
Early forensic tools, like MACE and Norton, provided basic recovery abilities, such as undelete and unformat. Most investigations were on a single workstation that was used by one individual. The open-source, community-driven model that is used today for digital forensic tool development makes tool evolution modular, extensible, robust and sustainable, across various platforms. Software and standards baselines provide a foundation that focuses on extensions, plug-ins and digital evidence bag (DEB) metaformat for development.

Government involvement in standardizations began in 1984, when the FBI established the Computer Analysis and Response Team (CART) to meet the growing demands of law enforcement for a more structured approach to examine evidence. By the early 1990s, the FBI was assisting the US Postal Service in creating its own computer forensics unit. A group of federal crime laboratory directors, which became the Scientific Working Group on Digital Evidence (SWGDE), began meeting twice a year to discuss areas of mutual interest. After Mark Pollitt, Unit Chief of CART, spoke to the directors about digital evidence and Scott Charney, CCIPS, discussed legal aspects of computer evidence and search warrant requirements for seizing digital evidence, another technical working group (TWG) was formed to address the forensic issues that are related to digital evidence. In the United Kingdom, the needs of law enforcement led to the creation of the National Hi-Tech Crime Unit in 2001, with resources that are centralized in London. The unit became the Serious Organised Crime Agency (SOCA) in 2006.

Following are further developments in digital forensics:

- **1993**—The first International Conference on Computer Evidence was held in the United States.
- **1995**—The International Organization on Computer Evidence (IOCE) was formed.
- **1998**—G8 appointed IOCE to create international principles, guidelines and procedures for digital evidence and the INTERPOL Forensic Science Symposium, to respond to issues in computer forensics. With the advent of cases admitting digital evidence in court, there was a need for standardization.
- **2002**—The SWGDE published “Best practices for Computer Forensics.”
- **2004**—The Budapest Convention on Cybercrime, which was signed in 2001, became effective. The convention worked to reconcile national computer crime laws, investigative techniques and international cooperation. The Convention was the first international treaty on crimes committed via the Internet and other computer networks, focusing on infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network security. The United States was the sixteenth country to ratify the Convention in 2006.
- **2005**—The International Organization for Standardization (ISO) published ISO 17025, General requirements for the competence of testing and calibration laboratories.

---


In 2013, US President Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, which calls for a voluntary risk-based cybersecurity framework (the Cybersecurity Framework, or CSF) that is “prioritized, flexible, repeatable, performance-based, and cost-effective.” The National Institute of Standards and Technology (NIST) led the development of the CSF through an international partnership of organizations, including owners and operators of the nation’s critical infrastructure and ISACA. Key principles from the ISACA COBIT 5 business framework, which helps enterprises to govern and manage their information and technology, are embedded into the CSF.

*Implementing the NIST Cybersecurity Framework* guide implements the CSF using ISACA’s COBIT 5 processes. In the CSF, digital forensics is a subcategory in the Respond function and Analysis category of the Framework Core. The study guide for the ISACA Cybersecurity Fundamentals Certificate discusses digital forensics in the incident responses topic.

**TYPES OF INVESTIGATIONS**

Although cybercrime activity and security breaches continue to rise, business requirements often take precedence over security requirements. This precedence leaves applications, systems and networks vulnerable to intrusion. When a breach occurs, the forensic analyst must locate the point of compromise. The mission criticality of the compromised application, system or network determines the level of investigation. A full forensic examination is less likely on a highly critical system because the system cannot be shut down or slowed down to do a full backup.

The two types of computer crime investigations are computer-based crime and computer-facilitated crime. In a computer-based crime, a computer or computers are used as the vehicle to commit a crime. In computer-facilitated crime, a computer is the target of a crime (e.g., a hacking incident or theft of information).

Computer-based crimes are activities such as child pornography, cyberbullying, cyberstalking, spamming or cyberterrorism. Typically, computers and/or hard drives are seized as evidence and provided to a forensic expert to analyze. When a computer has been the target of a crime, usually the information system is compromised, and information on the system or network is stolen, or fraudulent documents are created. Digital forensics is used to capture volatile information from random access memory (RAM) and other running processes, including networks. It is important for the forensic expert to consider the following four areas of analyses:

- Storage media
- Hardware and operating systems
- Networks
- Applications
RELEVANT LAWS
In any investigation, it is important to consult with a legal counsel on the applicability of local, regional, national and international laws. In the United States, the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030, criminalizes conduct that abuses computer systems. The statute protects computers that have a federal interest, i.e., federal computers, financial systems and computers that are used in interstate and foreign commerce. The statute protects computer systems from trespass, threats, damage, espionage and being used as tools of fraud.

Other statutes that may apply follow:12

- **The Interception of Communications:** 18 U.S.C. § 2511(1)(a) & (b); the disclosure of intercepted communications, 18 U.S.C. §2511(1)(c) & (e); and the use of intercepted communications, 18 U.S.C. § 2511(1)(d). These prohibitions are subject to a number of exceptions, most of them detailed in section 18 U.S.C. § 2511(2).

- **Unlawful Access to Stored Communications:** 18 U.S.C. § 2701; Section 2701 focuses on protecting email and voice mail from unauthorized access.

- **Aggravated Identity Theft:** 18 U.S.C. § 1028A, The Identity Theft Penalty Enhancement Act, which took effect July 15, 2004, established a new offense of aggravated identity theft. Section 1028A applies when a defendant “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.”

- **Access Device Fraud:** 18 U.S.C. § 1029. Ten separate activities relating to access devices are criminalized in 18 U.S.C. § 1029. The term “access device” is defined as any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).


- **Wire Fraud:** 18 U.S.C. § 1343 provides: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits, or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial 110 Prosecuting Computer Crimes institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

- **Communication Interference:** 18 U.S.C. § 136. Where a compromised computer is owned or used by the United States for communications purposes, 18 U.S.C. § 1362 may provide an alternative or additional charge.

- **Title 18:** United States Code, Section 1362 provides: Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.

---

For a more comprehensive reading of applicable US federal laws, Prosecuting Computer Crimes is available for download from the Department of Justice.\textsuperscript{13} State statutes should also be considered, and consulting with a legal counsel is advised. Additional US laws\textsuperscript{14} include the following:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Consumer Credit Protection Act
- Telephone Records and Privacy Protection Act

Internationally, the European Union (EU) developed a working document that pertains to the identification and handling of electronic evidence. The EU/Council of Europe (COE) Joint Project on Regional Cooperation against Cybercrime: Electronic Evidence Guide is a basic guide for law enforcement and judges.\textsuperscript{15}

US law enforcement personnel who search and seize computers during an investigation should be aware of the requirements in the Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual, from the Department of Justice Computer Crime and Intellectual Property Section.\textsuperscript{16}

\section{Digital Forensics Policies and Set of Controls}

The enterprise cybersecurity program should have policies that address all forensics considerations, such as contacting law enforcement, monitoring, and conducting regular reviews of forensics policies, guidelines and procedures. Good practice requires that policies are part of an overall governance and management framework, such as COBIT 5, from ISACA, which provides a hierarchical structure into which all policies should fit and link clearly to the underlying principles.\textsuperscript{17} Policies should be aligned with the enterprise risk appetite, which is determined in the risk governance activities, and are a key component of the enterprise system of internal control.\textsuperscript{18} Policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons in appropriate circumstances. The policies should clearly define the roles and responsibilities of all people who perform or assist with the enterprise forensic activities.\textsuperscript{19} Policies, guidelines and procedures should clearly identify the tools that may be used in a forensic review and provide reasonable guidance on the use of those tools under various circumstances.

Note: Information security and cybersecurity require a comprehensive set of controls. The set of controls, audit category and reviews for cybersecurity investigations and forensics are explained in detail in the ISACA publication Transforming Cybersecurity.\textsuperscript{20} This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity into a business process in a systemic way.
Many cyberincidents can be handled more efficiently and effectively if forensics considerations are incorporated into the information system life cycle. Examples of such considerations follow:

- Perform regular backups of systems and maintain previous backups for a specific period of time.
- Enable auditing on workstations, servers and network devices.
- Forward audit records to secure centralized log servers.
- Configure mission-critical applications to perform auditing and include the recording of all authentication attempts.
- Maintain a database of file hashes for the files of common operating system and application deployments, and use file integrity checking software on particularly important assets.
- Maintain records (e.g., baselines) of network and system configurations.
- Establish data retention policies that support the performance of historical reviews of system and network activity, comply with requests or requirements to preserve data that are related to ongoing litigation and investigations, and destroy data that are no longer needed.

DIGITAL FORENSICS SCIENTIFIC PROCESS

Ken Zatyko, the former director of the Defense Computer Forensics Laboratory, defined the following eight-step digital forensics scientific process:

1. Obtain search authority—In a legal investigation, legal authority is required to conduct a search or seizure of data.
2. Document chain of custody—In legal contexts, chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct.
3. Image and hash—When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.
4. Validate tools—When possible, tools that are used for forensics should be validated to ensure reliability and correctness.
5. Analyze—Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.
6. Repeat and reproduce (quality assurance)—The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts.
7. Report—The forensic analyst must document his/her analytical procedure and conclusions for use by others.
8. Possibly present expert testimony—In some cases, the forensic analyst will present his/her findings and conclusions to a court or another audience.

The process involves more than intrusion-related security incidents. Zatyko defines scientific digital forensics as:

“The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.”

As the process steps indicate, the digital forensic analyst meticulously handles, analyzes and reports on the evidence obtained, to present an objective opinion on the facts of a case without prejudice.
APPLYING VARIATIONS OF THE SCIENTIFIC METHOD
Scientists often use variations of the scientific method to solve problems. **Deductive reasoning** applies broad principles to predict specific answers (see figure 2). Conversely, **inductive reasoning** uses a series of specific pieces of information to extrapolate a broad conclusion. For example, forensic analysts might use inductive reasoning to determine where a cyberincident started.

Because physical evidence may never depict all the events that happened, inductive reasoning has a greater level of uncertainty. The conclusions are based on limited information rather than on a more solid scientific principle, but inductive reasoning can be useful when no broad principle can be applied. **The forensic analyst identifies the best tools and approach for each case.**

Digital forensics follows a rigorous scientific process to present findings of fact to prove or disprove a hypothesis in a court of law, civil proceeding or another action. Zatyko’s eight-step process can be grouped into three basic steps: acquisition, analysis and reporting, which are discussed in the following paragraphs and shown in figure 3.

---

**Variations of the Scientific Method of Forensic Science**

<table>
<thead>
<tr>
<th>Inductive Reasoning</th>
<th>Deductive Reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation</td>
<td></td>
</tr>
<tr>
<td>Experiment</td>
<td></td>
</tr>
<tr>
<td>Generalizations</td>
<td>Predictions</td>
</tr>
<tr>
<td>Paradigm/Theory</td>
<td></td>
</tr>
</tbody>
</table>

Source: Forensics: Examining the Evidence, “Understanding the Scientific Method,”
www.forensicbasics.org/science-law/what-constitutes-science/understanding-the-scientific-method

---

DATA COLLECTION

The acquisition of data begins with seizure, imaging or collection of digital evidence to capture suspect media or network traffic and logs, post breach. Enterprises typically assume that they have the right to monitor their internal networks and investigate their own equipment as long as they observe the privacy right of the employee. Employee privacy rights and the enterprise rights should be in written policies that are communicated to employees. In the United States, the Fourth Amendment covers seizures. Federal warrants are issued under Title 18 of the US Code for probable cause of a crime. However, exceptions allow data collection without a warrant for reasons such as consent, hot pursuit or plain view. In the United Kingdom, a magistrate issues warrants to a constable under Section 18 of the Police and Criminal Evidence Act. In the US, no one should ever go on site until after they read the search warrant to review the seizure authority and the affidavit for the reasoning and the items to be seized. Regardless of the country, enterprises should understand and follow local and country jurisdiction laws before seizing materials.

After digital media are acquired, an exact duplicate image (the forensic image) of the original media evidence is created and validated with hash values that have been calculated for the original digital media and the duplicate image. A hashing function, e.g., MD5, SHA-1 and SHA-256, applies a mathematical algorithm to the digital data and returns a fixed-size bit string hash value. Any change to the data will change the hash value. Data with the same hash value are identical. The hash value validates that the evidence is still in the original state. The original media evidence is write blocked and stored to prevent any further possible alteration. Hashing may not always be possible. Mobile devices and memory, in particular, may have to be treated differently to maintain evidence.
EXAMINATION AND ANALYSIS
After the duplicate image of the evidence is created, analysis can begin on the image. The digital forensic analyst may use specialized tools to uncover deleted or hidden material. Depending on the forensic request, the analyst can report findings about numerous types of information, e.g., email, chat logs, images, hacking software, documents and Internet history. After evidence is collected and analyzed, it is assembled to reconstruct events or actions and provide facts to the requesting party. These facts may identify people, places, items and events and determine how they are related so that a conclusion can be reached. This effort can include correlating data among multiple sources. In some environments, early case assessment (ECA) provides immediate review for the requesting parties, at which time they can ask for more advanced analysis. ECA typically involves imaging, indexing, archiving and an internal reporting mechanism for the requesting party to quickly access needed reconnaissance. ECA typically saves time and is often preferred over analysis.

REPORTING
After the analysis is complete, a report of the findings is developed, which outlines findings and methodologies. The provided exhibits may include attribution of file ownership, chat logs, images and emails; detailed login/logoff times; entry into facility logs and anything that places the suspect at the device at the same time and location of an event. The findings can be used to confirm or disprove alibis and provided statements. Digital evidence can also be used to prove intent. The completed report is given to the investigator, who is usually from law enforcement in a criminal matter or a designated senior manager in a civil action. Further actions are determined after the report is reviewed.

Digital forensic analysts provide facts and impart knowledge to give expert opinion only when they are required to do so in court. They never seek to aid or blame. Instead, analysts provide a scientific basis so that the court, company or other requesting party may use the unbiased evidence and gain a better understanding of events.

BRANCHES OF DIGITAL FORENSICS
Computer forensics is the oldest and most stable discipline of digital forensics. It concentrates on developing evidence from a computer and associated digital storage devices in a forensically sound manner to preserve, develop, recover when necessary, analyze and present facts in a clear and concise manner. In computer forensics, after the storage device is acquired, it is standard practice for an analyst to create a disk image from which to work. If the original device is confiscated, it is safely stored as evidence. Sometimes a device is not confiscated so that additional evidence can be gathered and future activities can be monitored. The forensic analyst creates a disk image of the device to preserve the original evidence. Today, virtual drives may also be used as way to emulate an entire machine.

A number of techniques are used in computer forensics investigations. Cross-drive analysis correlates information that is found on multiple hard drives, which are being used to identify social networks. Live analysis extracts dates using existing system administration or developed forensic tools. Recovering deleted files is often in the news, and it remains a mainstay of forensics for recovering evidence. Because files are not erased, but are overwritten eventually, over a period of time, an analyst has time to reconstruct deleted files.
Network forensics is a relatively new field within digital forensics. Generally, network forensics focuses on monitoring and analyzing computer network traffic to gather evidence of exceeding authorization or detect an intrusion from a party with no authorization to be on that system or network. Because network traffic is volatile and dynamic, analysts must be proactive in their approach to capturing information. Network forensics takes two approaches to gathering information:

- The more traditional approach catches and stores all data for analysis at a later time (e.g., logging the Internet usage of all users and only reviewing the data after an alert).
- The second approach scans the data that pass through the network and is selective about the data that are captured (e.g., only logging blocked sites and specific file formats from user activity).

The benefit of the first approach is that the analyst has all the information, but the negative aspect is that a large amount of archival storage space is needed and analysis is done later. In the second approach, the analyst does not need to waste time filtering, but the approach requires faster processing speed to manage incoming network traffic. Because data gathering is minimized, the likelihood of private or sensitive information being captured is substantially reduced. Digital forensic analysts can review network communications from obscure sources such as BitTorrent clients, PlayStation® and Xbox® game consoles, and Raspberry Pi. Network forensics continues to grow, due to the popularity of wireless communication, obfuscated communication (e.g., Tor anonymity software), and mobile devices.

Mobile device forensics roots began when mobile devices started to become popular, about 2000. Forensics of mobile devices includes cell phones, but can also include Universal Serial Bus (USB) drives, personal digital assistants (PDAs), global positioning systems (GPSs), cameras and tablet devices. From a law enforcement prospective, these data sources may provide a wealth of personal information, such as contacts, emails, web browsing information, photos, videos, calendars, geolocation, and social network messages and contacts. Mobile devices present greater challenges in handling due to memory volatility, so proper handling procedures must be followed to protect digital data. Most mobile devices have a basic set of comparable features and capabilities. They house a microprocessor, read-only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The operating system of a mobile device may be stored in either NAND or NOR memory, while code execution typically occurs in RAM. Generally, the information collected comes from internal memory (flash memory) or external memory (subscriber identity module [SIM], Secure Digital [SD], MultiMediaCard [MMC], CompactFlash [CF] cards or memory sticks). Call records and mobile backups can also be obtained through carriers, which provide other information that is useful in developing evidence, especially in cases of encryption. For a more complete understanding of techniques for handling mobile devices, NIST SP 800-101, Guidelines on Mobile Device Forensics and the SWGDE “Best Practices for Mobile Phone Forensics” should be reviewed.

Encryption has become the standard on Windows® 8.1, Mac® OSX 10.9, and will continue to be a challenge in the field. Circumventing encryption can involve a few steps, including memory capture for passwords in RAM, password cracking of a system image, interrogating the suspect or obtaining a search warrant for a mobile backup of a phone from a service provider. There are endless ways to defeat encryption, but forensic analysts must be willing to evolve with technology. This may include the biggest taboo in the field: modifying the user’s data in order to obtain said encryption keys. Memory forensics is too large a topic to be discussed here, but previewing applications and obtaining data from RAM leaves a footprint. Having a standardized process and taking copious notes are just two ways to justify actions in the field, but this does not erase the blurred lines.

---

27 Ibid.
Digital forensics is a growing field with much diversity in the technologies in which a professional can specialize. From the early stages of digital forensics, when evidence was collected from a stand-alone machine, to the highly networked cloud and mobile environment of today, digital forensic analysts have always taken great care while handling and preserving electronic information. Developing a step-by-step approach to preserve information for each new type of technology has evolved along with the field. The National Academy of Science recently identified digital forensics as a subfield within cybersecurity. As Scott Charney, head of the Department of Justice, Computer Crimes and Intellectual Property Section (CCIPS), stated, “The Internet crime problem is going to get worse. How do I know? Simple. There is always a percentage of the population who are up to no good. As the entire population moves to the Internet, so will the criminals.”

Note: Because not all aspects of the digital forensics field could be covered in this paper, such as eDiscovery and anti-forensics techniques, the reader can explore the field further to gain a wider knowledge of digital forensics.
ISACA®

With more than 115,000 constituents in 180 countries, ISACA (www.isaca.org) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. The association has more than 200 chapters worldwide.

Disclaimer

ISACA has designed and created Overview of Digital Forensics white paper (the “Work”) primarily as an educational resource for security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.
ACKNOWLEDGMENTS

Expert Reviewers
Jaime Buzzeo, USA
Joel Valverde, USA
Alexander Applegate, USA

ISACA Board of Directors
Robert E Stroud
CGEIT, CRISC, CA, USA, International President
Steven A. Babb
CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes
CISA, CISM, CGEIT, CRISC, BAE Systems Detica, Australia, Vice President
Robert A. Clyde
CISM, Clyde Consulting LLC, USA, Vice President
Rameses Gallego
CISM, CGEIT, CCSP, CISSP, Six Sigma Black Belt, Delt, Spain, Vice President
Theresa Grafenstine
CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj
CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski
CISA, SABIC, Saudi Arabia, Past International President
Debbie A. Lew
CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam
CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis
CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board
Steven A. Babb
CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato
CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow
CISA, CISM, CRISC, CISSP,
Capital One, UK
Charlie Blanchard
CISA, CISM, CRISC, CISSP, CIPP/US, CIPP/E, CISSP, FBICS, ACA, Amgen Inc., USA
Sushil Chatterji
CGEIT, EduTech Enterprises, Singapore
Phil J. Lageschulte
CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble
CISA, Vrije University, USA
Jamie Pasfield
CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez
CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Cybersecurity Task Force
Eddie Schwartz
CISA, CISM, CISSP, MCSE, PMP, USA, Chairman
Manuel Aceves
CISA, CISM, CGEIT, CRISC, CISSP, FCITSM, Cerberian Consulting, SA de CV, Mexico
Sanjay Bahl
CISM, CISSP, India
Neil Patrick Barlow
CISA, CISM, CRISC, CISSP, Capital One, UK
Brent Conran
CISA, CISM, CRISC, CISSP, Capital One, UK
Derek Grocke
HAMBS, Australia
Samuel Linares
CISA, CGEIT, CRISC, CISSP, GICSP, Industrial Cybersecurity Center (CCI), Spain
Marc Sachs
Verizon, USA