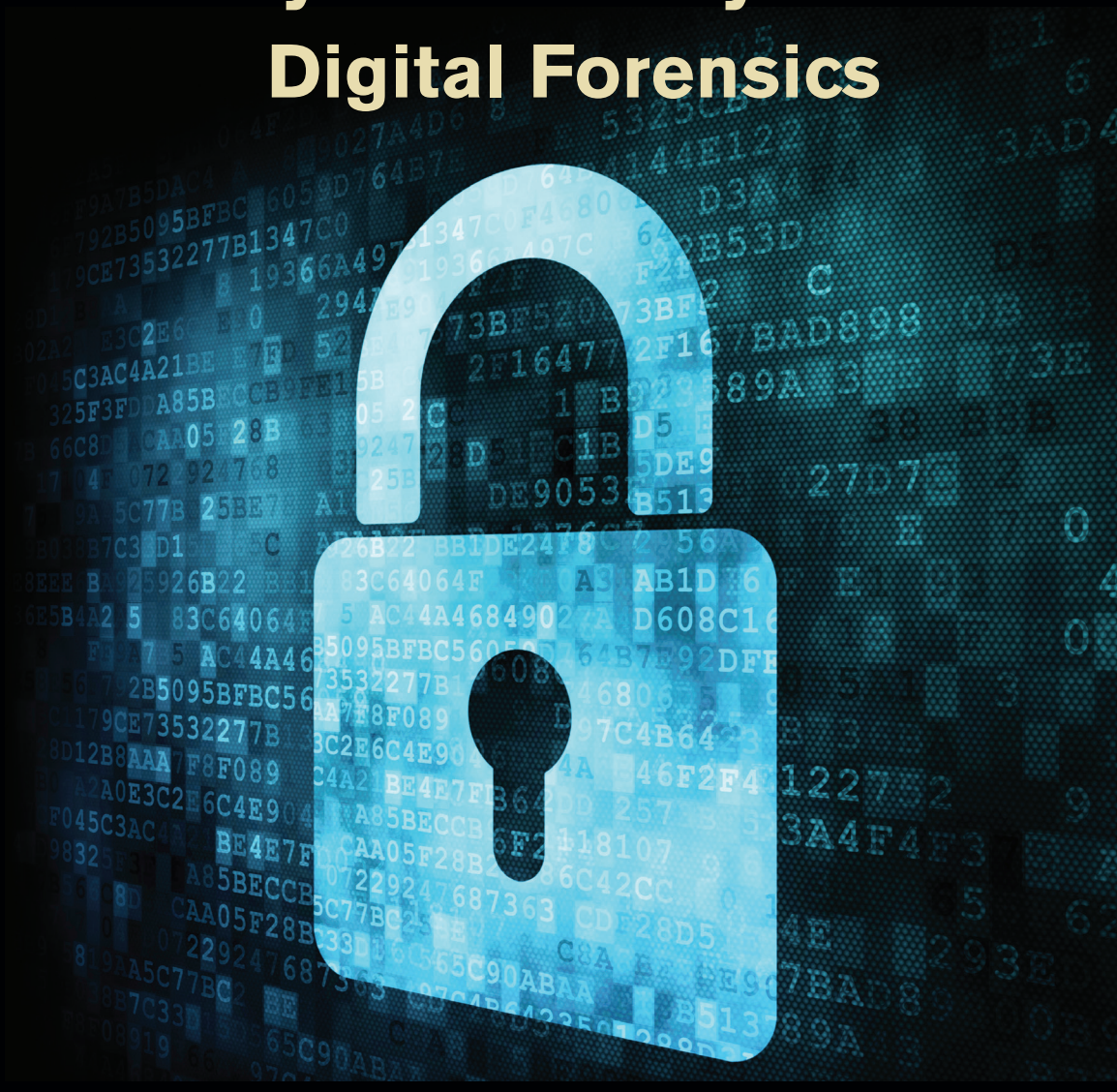
WHAT EVERY ENGINEER SHOULD KNOW

# What Every Engineer Should Know About Cyber Security and Digital Forensics



CRC Press
Taylor & Francis Group

Joanna F. DeFranco

# What Every Engineer Should Know About Cyber Security and Digital Forensics

# WHAT EVERY ENGINEER SHOULD KNOW
# A Series

Series Editor*

**Phillip A. Laplante**

*Pennsylvania State University*

1. What Every Engineer Should Know About Patents, *William G. Konold, Bruce Tittel, Donald F. Frei, and David S. Stallard*
2. What Every Engineer Should Know About Product Liability, *James F. Thorpe and William H. Middendorf*
3. What Every Engineer Should Know About Microcomputers: Hardware/Software Design, A Step-by-Step Example, *William S. Bennett and Carl F. Evert, Jr.*
4. What Every Engineer Should Know About Economic Decision Analysis, *Dean S. Shupe*
5. What Every Engineer Should Know About Human Resources Management, *Desmond D. Martin and Richard L. Shell*
6. What Every Engineer Should Know About Manufacturing Cost Estimating, *Eric M. Malstrom*
7. What Every Engineer Should Know About Inventing, *William H. Middendorf*
8. What Every Engineer Should Know About Technology Transfer and Innovation, *Louis N. Mogavero and Robert S. Shane*
9. What Every Engineer Should Know About Project Management, *Arnold M. Ruskin and W. Eugene Estes*
10. What Every Engineer Should Know About Computer-Aided Design and Computer-Aided Manufacturing: The CAD/CAM Revolution, *John K. Krouse*
11. What Every Engineer Should Know About Robots, *Maurice I. Zeldman*
12. What Every Engineer Should Know About Microcomputer Systems Design and Debugging, *Bill Wray and Bill Crawford*
13. What Every Engineer Should Know About Engineering Information Resources, *Margaret T. Schenk and James K. Webster*
14. What Every Engineer Should Know About Microcomputer Program Design, *Keith R. Wehmeyer*
15. What Every Engineer Should Know About Computer Modeling and Simulation, *Don M. Ingels*
16. What Every Engineer Should Know About Engineering Workstations, *Justin E. Harlow III*
17. What Every Engineer Should Know About Practical CAD/CAM Applications, *John Stark*
18. What Every Engineer Should Know About Threaded Fasteners: Materials and Design, *Alexander Blake*
19. What Every Engineer Should Know About Data Communications, *Carl Stephen Clifton*
20. What Every Engineer Should Know About Material and Component Failure, Failure Analysis, and Litigation, *Lawrence E. Murr*
21. What Every Engineer Should Know About Corrosion, *Philip Schweitzer*
22. What Every Engineer Should Know About Lasers, *D. C. Winburn*
23. What Every Engineer Should Know About Finite Element Analysis, *John R. Brauer*

*Founding Series Editor: William H. Middendorf

# What Every Engineer Should Know About Cyber Security and Digital Forensics

Joanna F. DeFranco

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742


Version Date: 20130927

International Standard Book Number-13: 978-1-4665-6454-1 (eBook - PDF)

*This book is dedicated to my husband, Michael Tommarello, and our children, Michaela, Marisa, and Nina, for their love, support, and continuous encouragement.*

# *Contents*

# *What Every Engineer Should Know: Series Statement*

What every engineer should know amounts to a bewildering array of knowledge. Regardless of the areas of expertise, engineering intersects with all the fields that constitute modern enterprises. The engineer discovers soon after graduation that the range of subjects covered in the engineering curriculum omits many of the most important problems encountered in the line of daily practice—problems concerning new technology, business, law, and related technical fields.

With this series of concise, easy-to-understand volumes, every engineer now has within reach a compact set of primers on important subjects such as patents, contracts, software, business communication, management science, and risk analysis, as well as more specific topics such as embedded systems design. These are books that require only a lay knowledge to understand properly, and no engineer can afford to remain uninformed of the fields involved.

# *Preface*

Long gone are the days where the security of your critical data could be protected by security guards, cipher locks, and an ID badge worn by all employees. As the computing paradigm is continually changing with shared resources and mobility, firewalls and antivirus software are also not enough to protect critical assets. This book will cover topics that range from the processes and practices that facilitate the protection of our private information and critical assets from attack, destruction, and unauthorized access to the processes and practices that enable an effective response if and when the attacks, destruction, and unauthorized access occur. This book will provide information on those topics via real situations, case law, and the latest processes and standards from the most reliable sources. The goal is not for you to become a fully trained security or digital forensic expert (although I will explain how to accomplish that); rather, it is to provide accurate and sufficient information to pique your interest and to springboard you onto the right path if this is an area you wish to pursue. If you are not aiming to be the next security professional at your company, this book can assist you in understanding the importance of security in your organization because whether you are designing software, have access to personal data, or manage the day-to-day activities in your office, you need to take a part in protecting those critical assets. In any case, I am hoping the book will give you a new appreciation for the world of cyber security and digital forensics.

There are three main goals of this book. The first goal is to introduce the cyber security topics every engineer should understand if he or she uses a computer or a mobile device connected to the Internet. It is important to understand these topics, as most engineers work for organizations that need their data secure, and, unfortunately, not every organization invests in training its employees to understand how to reduce the risk of security incidents. It is a well-known fact that the weakest link in any system is the user. Just ask any hacker. The second goal is demonstrating the application of the security concepts presented. This will be accomplished by presenting case studies of real-world incidents. The final goal is to provide information on certifications in the areas of cyber security and digital forensics for the reader who wants to break into this exploding field.

# *Acknowledgments*

Many people provided invaluable support and assistance in various ways during the writing of this book. I want to take this opportunity to thank the following:

- Dr. Phillip Laplante, for his invaluable mentoring as well as allowing me to share our writing collaborations in this book
- Special Agent Kathleen Kaderabek, for her input regarding FBI training and the InfraGard organization, as well as for her comments on Chapter 6
- Jennifer Prescott, for doing an excellent job proofreading the manuscript
- Robert Maley, founder of Strategic CISO, for sharing his vast experience that contributed to the first two case studies in Chapter 7 and for his feedback on Chapter 5
- Keith J. Jones, senior partner at Jones Dykstra & Associates, for sharing his experience on the high-profile case *U.S. v. Duronio*
- Dr. Jungwoo Ryoo, for his review of and feedback on Chapter 3
- Allison Shatkin, editor, and Laurie Schlags, project coordinator, at Taylor & Francis, for their assistance and encouragement throughout this project
- My wonderful family members who help take care of my family while I am working: my parents, Joseph and Anna DeFranco; my in-laws, Joseph and Clara Tommarello; my sister-in-law, Ilana DeFranco; and my sister, Judy Mastrocola
- Gwen Silverstein, for providing a great example of acceptable use as well as being such an amazing listener on our daily runs

## Errors

Despite my best effort as well as the efforts of the reviewers and the publisher, there may be errors in this book. If errors are found, please report them to me at jfd104@psu.edu.

# *About the Author*

**Joanna DeFranco** is an assistant professor of software engineering and a member of the graduate faculty at Penn State University. She has held academic positions at New Jersey Institute of Technology and Cabrini College. Prior to her academic career, she spent many years as a software engineer for government and industry. Notable experiences during this period included traveling the world on naval scientific ships that collected data to make ocean floor maps and developing cable head-end products for Motorola. She has written many journal articles and contributed to conference proceedings on effective software and systems engineering problem solving, as well as digital forensics. She has also coauthored a project management book.

Dr. DeFranco is a certified computer forensics examiner (CCFE) and teaches computer and cyber forensics at Penn State. She also teaches courses on software engineering, project management, and problem solving, which have all had an influence on her perspective of cyber security and digital forensics. She is on the curriculum advisory board for computer forensics at Middle Bucks Institute of Technology and is a member of the American Society for Engineering Education (ASEE). She earned a BS in electrical engineering from Penn State, an MS in computer engineering from Villanova University, and a PhD in computer and information science from New Jersey Institute of Technology.

# 1

# *Security Threats*

> The United States strongly condemns the illegal disclosure of classified information. It puts people's lives in danger, threatens our national security, and undermines our efforts to work with other countries to solve shared problems.
>
> **—Hillary Clinton**

## 1.1 Introduction

If you use a computer that is connected to the Internet, your information is at risk. The Bureau of Justice Statistics (BJS) reported from interviewing 7,818 businesses, that 67 percent detected at least one cyber crime (Rantala 2008). Of the nearly 8,000-company sample, more than a third of them are *critical infrastructure* businesses. Nearly 60 percent reported a cyber attack to their computer system; 11 percent reported cyber theft, which includes embezzlement, fraud, and intellectual property theft; and 24 percent reported other cyber incidents such as port scanning, spyware,* spoofing,† or some type of breach that resulted in damage or a loss.

Even if you are not an engineer working at a business that is considered critical infrastructure or a company that has a more moderate risk level, you have an identity and personal information that you need to protect; thus, you need to be an informed computer user.

The Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), reports an average of 26,000 complaints a month (2011 Internet Crime Report). A few of the crimes reported include identity theft, crimes that target computer networks or devices, and scams where the criminal poses as the FBI to defraud victims. This implies that, you need to prepare yourself and your business for an attack—because it will happen eventually.

* Spyware is software that self-installs on one's computer with the goal of stealing personal information, usually for the purpose of determining Internet-browsing habits.

† Spoofing is impersonating an individual by forging an e-mail header.

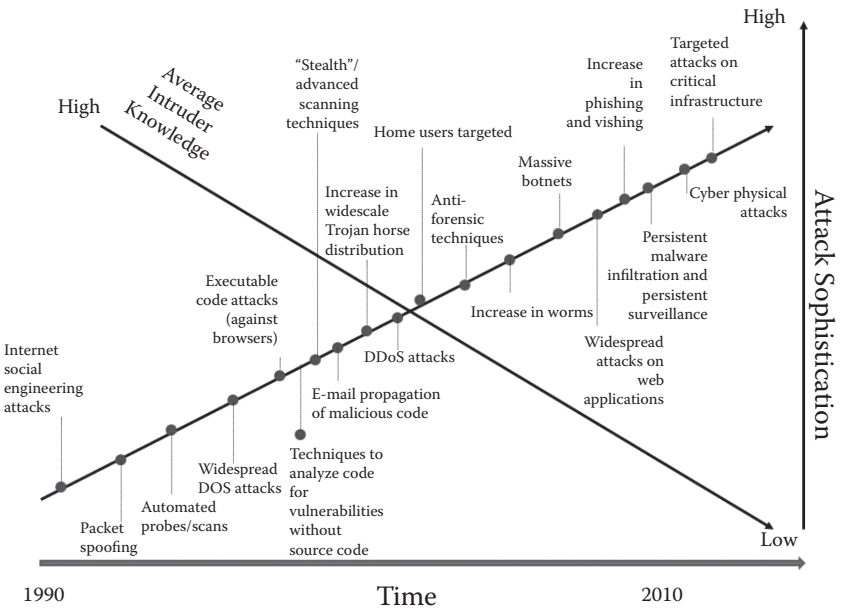



**FIGURE 1.1**
The trends in cyber attacks. (Adapted from Lipson, H., 2002, special report CMU/SEI-2002-SR-009, and Carnegie Mellon, 2010, http://www.cert.org/tces/pdf/archie%20andrews.pdf)

Why are these attacks so much more prevalent and sophisticated? Because, as shown in Figure 1.1, the technical knowledge required by the hacker is decreasing. The attacks listed only highlight a few types of vulnerabilities, but there are enough shown to verify the point that it does not take a PhD or twenty years of computer experience to hack into a computer. The FBI has knocked on the doors of many people who are the parents of the "model" teenager. In a particular case, the teenager who was known for just hanging out at home and using the family computer, but was actually hacking into NASA's computers.*

The focus and goal of this chapter are to highlight some of the common cyber security risks. We will start with the one that is the most difficult to defend against: social engineering. It is difficult to defend against because it preys on human nature to want to be helpful and kind. Once the social engineer finds a victim, he or she just needs to persuade (trick) the victim into revealing information that will compromise the security of the system.

* The first juvenile hacker to be incarcerated for computer crimes was 15 years old. He pled guilty and received a six-month sentence in jail. He caused a twenty one-day interruption of NASA computers, invaded a Pentagon weapons computer system, and intercepted 3,300 e-mails and passwords (Wilson, ABC News).

Cause for Paranoia?*

There is a reason for paranoia about the threat of cyber attacks. Consider the following:

- The ScanSafe Annual Global Threat Report recorded a 252 percent growth in attacks on banking and financial institutions, 322 percent growth in attacks on pharmaceutical and chemical industries, and 356 percent growth in attacks on the critical oil and energy sectors in 2009 (www.scansafe.com/downloads/gtr/2009_AGTR.pdf).
- More than half of the operators of power plants and other critical infrastructure suspect that foreign governments have attacked their computer networks (Baker 2010).
- Of those operators, 54 percent acknowledged they had been hit by stealthy infiltration—applications planted to steal files, spy on e-mails, and control equipment inside a utility (Baker 2010).
- At nearly 2,500 companies, such as Cardinal Health and Merck, 75,000 computer systems have been hacked by malicious "bots" that enabled the attacker to manipulate the user's computer and steal personal information (Nakashima 2010).

New threats are constantly being reported, largely on the infrastructure of only a few countries. The attacks on these systems often exploit vulnerabilities provided by unwary users—and we can all be "unwary users" at times.

## 1.2 Social Engineering

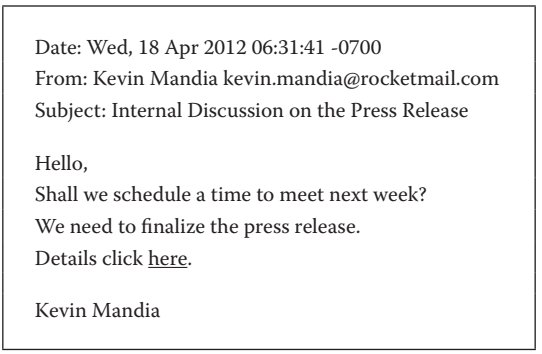
The greatest threat to the security of your business is the social engineer (Mitnick and Simon 2002). In other words, your company can employ the latest state-of-the-art security equipment and it will still be vulnerable due to the ignorance of the system's users. Essentially, the social engineer takes advantage of the weakest link in your company—the user (see Figure 1.2). They are able to obtain confidential information without the use of technology.

The confidential information obtained by the social engineer is used to perform fraudulent activities or gain unauthorized access to an computer system. As you can imagine, social networking has made social

* Excerpt from Laplante and DeFranco (2010).


**FIGURE 1.2**
The weakest link in the company. (Weiner, Z., 2012, Hacking. (http://www.smbc-comics.com/ [February 20, 2012].))

engineering even easier. In an interview with Kevin Mitnick, the person who made social engineering famous, he described using a "spear phishing" tactic where an e-mail targets a specific person or organization coming from a trusted source. The person is targeted using information found on a social networking site. For example, the social engineer goes to *LinkedIn* and looks for network engineers because they usually have admin rights to the network (Luscombe 2011). Then, he or she sends those network engineers an e-mail (since he or she knows where they work) or calls them to obtain the needed information. Even a company specializing in cyber attack recovery is a spear phishing target. In a report written by Mandiant (2013), a spear phishing attack was described targeting the company's CEO, Kevin Mandia. The goal was to attack the organization with


Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia kevin.mandia@rocketmail.com
Subject: Internal Discussion on the Press Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia

**FIGURE 1.3**
Spoofed e-mail. (Adapted from Mandiant APT1 report, 2013, www.mandiant.com.)

an advanced persistent threat (APT*). The spear phishing e-mail was sent to all Mandiant employees. The e-mail was spoofed to appear as if it came from the company's CEO, Mr. Mandia. The e-mail, shown in Figure 1.3, had a malicious APT attachment (notice the spoofed e-mail address: @ rocketmail.com).

To show you how easy a social engineering attack is, let us compare the steps a high-tech hacker and a no-tech hacker (social engineer) would use to get a password (Long 2008). As you read through the steps, keep in mind that it is estimated that the high-tech way takes about a week and the no-tech way takes merely a moment or two.

**A summary of the five-step high-tech way to obtain a password:**

1. *Strategically scan the company network:* In a stealthy manner (from several IP addresses) search for ports listening to the Internet.
2. *Install malware on a victim's machine:* Sneak the rootkit (malware) onto the open port.
3. *Enumerate the target network:* While continuing to hide your activity, determine the network topology; for example, the size of the network, number of switches, and the location of the servers.
4. *Locate and copy the encrypted password file:* Covertly take a copy of the network hashes to analyze on your own network. This may result in acquiring passwords.
5. *Run automated cracking tools against the encrypted password file:* Use the password hashes from step 4 with your favorite password cracking tool.

* An APT is an attack where hackers infiltrate the corporate network and steal sensitive data over a long period of time. APTs will be addressed in Chapter 4.

**A summary of the two-step no-tech way to obtain a password:**

1. *Make a phone call:* Ask easy questions. Find a way to swindle the person who answered the phone to reveal information such as terminology that only the insiders utilize. You may even be able to convince the person to provide you with access—which would eliminate step 2 of this process!
2. *Make another phone call:* In this conversation, use the information from the first phone call. You will now seem like one of them and the person on the other end will want to help you login! Essentially, one piece of information helps you get more information.

What needs to be understood at this point is that sensitive information can be obtained by just asking for it. In essence, social engineers take advantage of our human nature of kindness, which makes it easy for the social engineer to pretend to be someone else. Thus, when he or she is armed with a few pieces of information, more information to break into secure networks can easily be acquired.

In his book, *The Art of Deception,* Kevin Mitnick goes through story after story based on what he calls one of the fundamental tactics of social engineering: "gaining access to information that a company employee treats as innocuous, when it isn't" (Mitnick and Simon 2002). Social engineering tactics can only be countered by properly training the system users.

*News of the World* Mobile Phone Hacking Scandal

*News of the World,* a British tabloid, was put out of business after 168 years due to the ramifications of phone hacking allegations. The newspaper was accused of hacking the mobile phone voicemail of celebrities, politicians, members of the British Royal Family, and Milly Dowler, a murder victim. Hacking into Dowler's phone was considered evidence tampering, and the hackers could face about 500 civil claims (Sonne 2012). Most of the victims were hacked because the default PINs for remote voicemail access were never changed. Even if the user did change the PIN, the "hacker" used social engineering techniques to trick the operator into resetting the PIN (Rogers 2011).

## 1.3 Travel

Do you or your engineers travel abroad? Social engineering can also occur when traveling. Businesspeople, US government employees, and contractors

**TABLE 1.1**

Sensitive Information Targeted by Foreign Collectors

| **Critical Business Information May Include** | |
|---|---|
| Customer data | Phone directories |
| Employee data | Computer access protocols |
| Vendor information | Computer network design |
| Pricing strategies | Acquisition strategies |
| Technical components and plans | Investment data |
| Corporate strategies | Negotiation strategies |
| Corporate financial data | Passwords (computer, phone, accounts) |

*Source:* US Department of Justice, Federal Bureau of Investigation, n.d., business travel brochure.

that are traveling abroad are routinely targeted for a variety of sensitive information, shown in Table 1.1.

The targeting takes many forms, according to the "Report to Congress on Foreign Economic Collection and Industrial Espionage":

- Exploitation of electronic media and devices
- Secretly entering hotel rooms to search
- Aggressive surveillance
- Attempts to set up romantic entanglements

The exploitation could simply occur through software updates while using a hotel Internet connection (FBI E-scams 2012). A pop-up window will appear to update software while the user is establishing an Internet connection in the hotel room. If the pop-up is clicked, the malicious software is installed on the laptop. The FBI recommends either performing the upgrade prior to traveling or going directly to the software vendor's website to download the upgrade. All of these threats can be mitigated by training, as will be discussed in Chapter 4.

## 1.4 Mobile Devices

Many people use mobile devices to conduct business. As smartphones have become more prevalent, the hackers have taken notice. McAfee reports an increase of mobile threats from approximately 2,000 in 2011 to more than 8,000 threats in 2012. Part of the reason for the increase lies in McAfee's ability to detect these threats, but nonetheless, that is a significant amount of malware. At this point, most of the malware, usually contained in phone apps, targets the Android operating system because of the open-source

environment. The Android OS has been targeted because it does not provide adequate control over the private data, which are misused by third-party smartphone apps (Enck et al. 2010). Researchers at Penn State, Duke, and Intel Labs (2010) created an app called TaintDroid to monitor the behavior of third-party smartphone applications. They found that, out of 30 popular Android apps, there were 68 instances of private information misuse across 20 of the apps. For example, an innocent wallpaper app of a favorite character will send your personal information to China (Mokey 2010). There is a lot of pressure on developers to produce more functionality faster and at lower cost, which limits the time needed to improve mobile security (Hulburt, Voas, and Miller 2011). This is not to discourage smartphone use or app development, but rather to encourage awareness of the risks when downloading apps to your smartphone.

Is your iPhone a spiPhone? Researchers at Georgia Tech discovered how to use the smartphone accelerometer to sense computer keyboard vibrations and can decipher typing with 80 percent accuracy. The accelerometer is the internal device that detects phone tilting (Georgia Tech 2011). A possible attack scenario could be the user downloading a seemingly harmless application that includes the keyboard-detection malware. So, do not set your phone too close to your keyboard! Placing your phone 3 or more inches away from your keyboard is recommended.

## 1.5 Internet

The Internet is both a benefit and a detriment: It created a global transformation of our economy, but also threatens our privacy. According to McAfee Labs (2012), the amount of known malware application is over 80 million and continues to grow. The usual problems are, of course, fake antivirus (alerting victims of threats that do not exist), AutoRun (exploits mostly via USB), and password stealing (malware monitoring keystrokes). But, of greatest concern are rootkits which provide stealthy remote access to live resources and remain active for long periods on your system.

The FCC's chairman, Julius Genachowski, has stated that the three top cyber threats are botnets, domain name fraud, and Internet protocol route hijacking (Grace 2012). Bot-infected computers are computers that are controlled by an attacker. A botnet is the collection of those computers that, according to the FCC, "pose a threat to the vitality and resiliency of the Internet and the online economy." Domain name fraud converts the domain name (e.g., www.google.com) to an incorrect IP address, thus sending the user to a website where fraudulent activity will probably occur. Internet protocol hijacking is where the Internet traffic is redirected through untrustworthy networks. Mitigation tactics to these threats will be discussed later in this book.

## 1.6 The Cloud

The cloud model shares resources such as networks, servers, storage, applications, and services. In other words, a cloud offers computing, storage, and software "as a service" (Buyya, Broberg, and Goscinski 2010). According to the National Institute of Standards and Technology (NIST), a federal agency that provides standards to promote US innovation and industrial competitiveness, there are four varieties of clouds (Mell and Grance 2011):

1. A *private cloud,* where a single organization shares the resource infrastructure exclusively
2. A *community cloud,* where the users of the cloud infrastructure are from different organizations that share the same concerns (e.g., all of the organizations may need to consider the same security regulations)
3. A *public cloud,* where almost anyone can utilize its resources
4. A *hybrid cloud,* where the preceding three varieties are combined and connected to enable data and application sharing

No matter which variety of cloud you utilize, clouds essentially provide three types of services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS); see Table 1.2.

In addition to these cloud services, there are cloud services, related to security and privacy such as monitoring and addressing malware, spam, and phishing problems that come through e-mail. The cloud model is great, especially for small businesses that would not be able to provide an expensive, effective infrastructure without spending a lot of money. However, instead of money, the hefty price tag is the risk that comes with sharing these types of resources.

The "Guidelines on Security and Privacy in Public Cloud Computing," published by NIST (Jansen and Grance 2011), discusses four fundamental concerns of the cloud. First is system complexity. This complexity brings with it a

**TABLE 1.2**

Cloud Services

| Service Class | Service Content |
|---|---|
| SaaS | Cloud applications |
| | *Examples: social networks, office applications, video processing* |
| PaaS | Cloud platform |
| | *Examples: programming, languages, frameworks* |
| IaaS | Cloud infrastructure |
| | *Examples: data storage, firewall, computation services* |

*Source:* Buyya, R. et al., 2010, *Cloud Computing Principles and Paradigms.* New York: John Wiley & Sons.

large playground for attackers. The cloud offers so many services and sometimes even nest and layer services from other cloud providers. Combining this complexity with the necessity of upgrades and improvement, unexpected interactions are created along with opportunities for hackers. The second concern is the fact that components and resources are shared unknowingly with other consumers. Your data are separated "logically," not "physically." This shared multitenant environment creates another opportunity for someone to gain unauthorized access. A good example is a security breach that occurred with Google Docs that allowed users to see files that were not "owned" or "shared" by them (Kaplan 2008).

The third concern is the fact that applications that were utilized from the company Intranet are now used over the Internet, thus increasing network threats. And finally, by utilizing a cloud model, you have given the control of your information to the people who manage the cloud. This loss of control "diminishes the organization's ability to maintain situational awareness, weigh alternatives, set priorities, and affect changes in security and privacy that are in the best interest of the organization" (Jansen and Grance 2011).

The IBM Trend and Risk Report for 2011 also recognized the vulnerability that cloud computing brings to your systems. They suggest that when thinking about the risk of using a cloud infrastructure, you should consider the following questions:

- Has your security team audited the practices of your partners?
- Are the practices consistent with yours?
- How confident are you in their execution?

Even with these risks, companies still consider a cloud infrastructure because there are a few advantages (Jansen and Grance 2011):

1. The cloud providers are able to have staff that is highly trained in security and privacy.
2. The platform is more uniform, thereby enabling better automation of security management activities such as configuration control, vulnerability testing, security audits, and patching.
3. With the amount of resources available, redundancy and disaster recovery capabilities are built in. They are also able to handle increased demands as well as contain and recover more quickly from cyber attacks.
4. Data backup and recovery can be easier because of the superior policies and procedures of the cloud provider.
5. The client of the cloud can be easily supported on mobile devices (laptops, notebooks, netbooks, smartphones, and tablets) because all of the heavy-duty computational resources are in the cloud.

6. The risk of theft and data loss is lowered (though not gone) because the data are maintained and processed at the cloud.

## 1.7 Cyber Physical Systems

Cyber physical systems (CPS) integrate cyber, computational, and physical components to provide mission-critical systems. Examples of systems are smart electricity grids, smart transportation, and smart medical technology. These systems are "smart" because they are able to collect and use sensitive information from their environment to have an effect on the environment. But, because of the vast applications of CPS and the integrated computers and networks, they are impacted by cyber security.

The CPS needs not only to be usable but also to be safe and secure because the loss of security for a CPS can "have significant negative impact including loss of privacy, potential physical harm, discrimination, and abuse" (Banerjee et al. 2011). The first step in securing a CPS system is being aware of the cyber attacks that may impact the system. The smart grid, for example, needs to include the following security properties (Govindarasu, Hahn, and Sauer 2012):

1. *Confidentiality* and protection of the information from unauthorized disclosure
2. *Availability* of the system/information where it remains operational when needed
3. *Integrity* of the system/information from unauthorized modification
4. *Authentication* prior to access by limiting access only to authorized individuals
5. *Nonrepudiation*, where the user or system is unable to deny responsibility for a previous action

CPS is relatively young; thus, as these systems are being designed, we need to keep in mind the necessary components to uphold the security properties.

## 1.8 Theft

You not only need to improve your security posture to protect against hackers, but you also need to monitor the activities of your own employees. It is difficult to imagine that someone you trusted enough to hire would steal

from you, but as we know this happens every day. Consider a situation where making and selling a specific food product contributes to most of a company's revenue. None of the company's competitors have been able to duplicate this product. Thus, the recipe is guarded and only a few people have access to it. One of the people that know this trade secret announces that she is leaving but gives the impression that she is retiring. However, her plan is to work for a competitor. The security team determined from analyzing her system activity that she had begun accessing confidential files and storing them on a flash drive in the weeks prior to her departure.

Another example was described in the "Report to Congress on Foreign Economic Collection and Industrial Espionage." In this situation, an employee downloaded a proprietary paint formula valued at $20 million that he planned to deliver to his new employer in China. Just recently it was discovered at the University of South Carolina Health and Human Services that an employee e-mailed himself over 200,000 patient records. These examples show that sometimes it is the authorized users who cause the data breaches. There are many ways to protect against theft, which will be discussed in Chapters 3 and 4.

In the Hewlett-Packard 2012 "Cyber Risk Report," researchers determined the risk trends for cyber security. For example, the number of new disclosed vulnerabilities had increased 19 percent from 2011. These come from every angle, such as web applications, legacy technology, and mobile devices. For example, the skyrocketing mobile device sales in 2012 brought with it a similar number of mobile application vulnerabilities. Mobile device applications alone have seen a 787 percent increase in vulnerability disclosures. Understanding a company's technical security risk begins with knowing how and where the vulnerabilities occur within the organization (Hewlett-Packard 2013).

## References

Baker, S. January 2010. In the crossfire: Critical infrastructure in the age of cyber war. McAfee, http://resources.mcafee.com/content/NACIPReport.

Banerjee, A., Venkatasubramanian, K., Mukherjee, T., and Gupta, S. 2012. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proceedings of the IEEE* 100 (1).

Buyya, R., Broberg, J., and Goscinski, A. 2010. *Cloud computing principles and paradigms.* New York: John Wiley & Sons.

Carnegie Mellon, Software Engineering Institute. November 2010. Trusted computer in embedded systems. http://www.cert.org/tces/pdf/archie%20andrews.pdf (accessed May 1, 2012).

Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., and Sheth, A. 2010. TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. OSDI.

FBI (Federal Bureau of Investigation). 2012. New e-scams & warnings. http://www.fbi.gov/scams-safety/e-scams (accessed May 24, 2012).

Georgia Tech. October 18, 2011. Smartphones' accelerometer can track strokes on nearby keyboards. http://www.gatech.edu/newsroom/release.html?nid=71506 (retrieved June 21, 2012).

Govindarasu, M., Hahn, A., and Sauer, P. May 2012. Cyber-physical systems security for smart grid. Power Systems Engineering Research Center, publication 12-02.

Grace, N. 2012. FCC Advisory Committee adopts recommendations to minimize three major cyber threats, including an anit-bot code of conduct, IP route hijacking industry framework and secure DNS best practices. http://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats (retrieved June 22, 2012).

Hewlett-Packard Development Company. March 2013. HP 2012 cyber risk report, white paper. http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0313.pdf (retrieved April 9, 2013).

Hulburt, G., Voas, J., and Miller, K. 2011. Mobile-app addiction: Threat to security? *IT Professional* 13:9–11.

IBM. September 2011. IBM X-Force 2011 mid-year trend and risk report. http://www-935.ibm.com/services/us/iss/xforce/trendreports/ (retrieved June 1, 2012).

Internet Crime Complaint Center. 2011. 2011 Internet crime report. http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf (retrieved December 28, 2012).

Jansen, W., and Grance, T. December 2011. Guidelines on security and privacy in public cloud computing. Special publication 800-144, http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Kaplan, D. 2008. Google Docs flaw could allow others to see personal files. *SC Magazine*, September 16, 2008, http://www.scmagazine.com/Google-Docs-flaw-could-allow-others-to-see-personal-files/article/116703/?DCMP=EMC-SCUS_Newswire (retrieved June 1, 2012).

Laplante, P., and DeFranco, J. 2010. Another ode to paranoia. *IT Professional* 12:57–59.

Lipson, H. 2002. Tracking and tracing cyber-attacks: Technical challenges and global policy issues. Special report CMU/SEI-2002-SR-009.

Long, J. 2008. *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing.* Burlington, MA: Syngress.

Luscombe, B. August 2011. 10 Questions for Kevin Mitnick. http://www.time.com/time/magazine/article/0,9171,2089344-1,00.html (accessed May 18, 2012).

Mandiant. January 2013. APT1 exposing one of China's cyber espionage units. www.mandiant.com (retrieved April 10, 2013).

McAfee Labs. 2012. Threats report: First quarter 2012. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf (retrieved June 22, 2012).

Mell, P., and Grance, T. September 2011. The NIST definition of cloud computing. Special publication 800-145, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mitnick, K., and Simon, W. 2002. *The art of deception.* New York: Wiley Publishing.

Mokey, N. 2010. Wallpaper Apps Swiped Personal Details off android Phones. *Digital Trends*, July 19, 2010. http://www.digitaltrends.com/mobile/wallpaper-apps-swiped-personal-details-off-android-phones/(accessed may 18, 2012).

Nakashima, E. 2010. More than 75,000 computer systems hacked in one of largest cyber attacks, security firm says. *Washington Post,* February 19, 2010.

Office of the Director of National Intelligence. October 2011. Foreign spies stealing US economic secrets in cyberspace—Report to Congress on foreign economic collection and industrial espionage. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (retrieved May 24, 2012).

Rantala, R. 2008. Cybercrime against businesses, 2005. Bureau of Justice Statistics special report, US Department of Justice, revised October 27, 2008.

Rogers, D. 2012. How phone hacking worked and how to make sure you're not a victim. nakedsecurity, July 8, 2012, http://nakedsecurity.sophos.com/2011/07/08/how-phone-hacking-worked/ (retrieved June 1, 2012).

Sonne, P. 2012. News Corp. Faces Wave of Phone-Hacking Cases. *Wall Street Journal,* June 1, 2012. http://online.wsj.com/article/SB10001424052702303640104577440060134799828.html (retrieved June 1, 2012).

US Congress. February 2004. Annual report to Congress on foreign economic collection and industrial espionage—2003, NCIX 2004-1003. http://www.fas.org/irp/ops/ci/docs/2002.pdf (retrieved May 24, 2012).

US Department of Justice, Federal Bureau of Investigation. n.d. Business travel brochure. http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure (retrieved May 24, 2012).

Weiner, Z. 2012. Hacking (http://www.smbc-comics.com/[2/20/12]).

Wilson, C. n.d. 15-Year-old admits hacking NASA computers. http://abcnews.go.com/Technology/story?id=99316&page=1 (retrieved June 17, 2012).

# 2

# *Cyber Security and Digital Forensics Careers*

> In the middle of difficulty lies opportunity.
>
> **—Albert Einstein**

## 2.1 Introduction

Julie Amero, a substitute teacher in Connecticut, lost her career and had her life turned upside down due to a malicious spyware application and the incompetence of security "professionals." The spyware was running on the classroom computer causing pornographic images to be shown. Julie innocently checked her personal e-mail using that classroom computer, left the room briefly, and upon her return saw, as did a few students, the pornography on the computer screen. The pornography pop-ups* were caused by spyware inadvertently installed when another user of that classroom computer downloaded a Halloween screen saver. Because of the school's amateur IT administrator, overreaction from a school principal, faulty forensic examination of the physical evidence, and false testimony from a computer forensics "expert," she was prosecuted and convicted (later overturned) of risk of injury to a minor.†

What we can take away from this case is the importance of having a *qualified* computer forensics‡ examiner acquiring and analyzing evidence in addition to having a *qualified* information security professional protecting the critical assets of the enterprise. This includes training the employees on the proper use of the company computers as well as what to do when an incident occurs. We will address all of these topics later in this book, but for now we will discuss the numerous career opportunities in the field of information and cyber security as well as describe how to become a qualified professional in this exploding field.

---

* A pop-up is a browser window that appears out of nowhere when a web page is visited. Sometimes the pop-ups are advertisements and sometimes they are malicious programs that will install the undesirable content to the machine upon clicking.

† The technical details of this case can be found in Eckelberry et al. (2007).

‡ Computer forensics is also known as digital forensics. The terms are used interchangeably in this book.

## 2.2 Career Opportunities

We are very fortunate that we can easily search for job opportunities on the Internet. I remember a time, not too long ago, where we only had access to the newspaper "want ads" when we were looking for a job. The downside of using the Internet to search for a job, however, is sorting through all of the information. It can be an overwhelming process—especially in the cyber security arena, due to relative newness of the profession and its many certifications and job titles for very similar positions. Here are a few pointers that will save you time when job searching in this field:

1. *Make your search general enough to include many opportunities:* There are many different job titles for the same job.
2. *Be familiar with many certifications:* A certification is obviously a plus; accordingly, some of the positions that require certifications may allow you to earn the certification within the first year of employment rather than having it at the start. Therefore, you could start looking for a job at the same time that you are working on the certification. If you already have a certification, note that the certifications advertised may be similar to the one you have. This will become clearer after you review the certification options later in this chapter. In addition, if you earned a degree that covers the tasks or knowledge domains listed in the job posting, the employer may not require a certification.
3. *Some positions require security clearances, fingerprinting, and/or polygraph tests:* They will note that requirement in the job description and would most likely provide the means to accomplish that requirement.

As I am sure you are aware and probably one of the reasons you picked up this book, there are a vast amount of opportunities available in this field. It is safe to say that the work is endless. The first thing you need to determine is your general interests and then the qualifications required to get your foot in the door. The information in this chapter will facilitate that process by providing an overview of the tasks, training, and the necessary knowledge to acquire these positions. This chapter is by no means an exhaustive review, but it is an excellent starting point to make sense of the immense amount of information out there regarding the cyber security and digital forensics professions.

The first challenge you will encounter is sorting through the many job titles of these positions. When I graduated with a BS in electrical engineering, there were two job titles: electronics engineer and electrical engineer. The job descriptions varied, but you did not find that out until you were at the interview! There really is no standard job title in this field, so I would not focus on

it much. Here are some of the MANY job titles you will come across during your search in the security field:

- *Information security job titles:* information security risk specialist, information security officer, information security specialist, information security analyst, data security specialist, information security architect, information security engineer, firewall engineer, malware analyst, network security engineer, director of security, security operations analyst, vulnerability researcher/exploit developer, security auditor, disaster recovery/business continuity analysis manager, data warehouse security architect, and penetration testing consultant
- *Digital forensic job titles:* emergency response managing consultant, computer forensics analyst, digital forensics technical lead, digital forensics engineer, cell phone forensics analyst, IT systems forensic manager, information security crime investigator/forensics expert, incident responder, computer crime investigator, intrusion analyst, and system, network, web, and application penetration tester

The purpose of each career outline coming up is to give you an idea of what that professional may be asked to do or know. There is definite overlap in some of the tasks for the jobs listed. For example, you will note that the information security field includes an understanding of computer forensics knowledge. This is because the information security professional has designed and implemented the infrastructure that the computer forensics professional is investigating when an incident occurs. The information security professional needs to understand that it is not only important to implement a secure environment but also to implement effective monitoring, logging, and surveillance so that when (not if) the inevitable incident occurs, the computer forensics professional(s) will be able to analyze the system data to determine what happened to facilitate the prevention of the next occurrence. Thus, the computer forensics professional will have the necessary skill set to determine what has been compromised and, more important, be able to identify, recover, analyze, and preserve evidence in a forensically sound manner so that it will be admissible in court if the incident turns out to be a criminal offense. This may not be determined until all the data are analyzed.

### 2.2.1 A Summarized List of "Information Security" Job Tasks

1. **Develop and maintain the company security policy:** Create an acceptable use policy (AUP) to reduce the potential for legal action from the users of the system. The AUP is a set of rules applied

that restrict the way the network may be used and monitored. For example, part of the AUP will address *general use and ownership* and will contain a statement similar to the following:

> While XYZ's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remain the property of XYZ. Because of the need to protect XYZ's network, management cannot guarantee the confidentiality of information stored on any network device belonging to XYZ (SANS Institute).

2. **Monitor compliance with information security goals, regulations, policy, and procedures:** This requires knowledge of industry standards: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Federal Information Security Management Act (FISMA), and North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP). For example, if you are working for an organization that deals with electronic health information (e.g., health plans, healthcare providers etc.), then this National Institute of Standards and Technology (NIST) publication on HIPAA should be followed: "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." The HIPAA Security Rule focuses on safeguarding electronically protected health records. Thus, all healthcare and partnering organizations and anyone creating, storing, and transmitting protected health information electronically need to comply. The 117-page document focuses on improving the understanding of HIPAA overall, understanding the security concepts, and refers readers to other relevant NIST publications to assist in the compliance effort (Scholl et al. 2008).

   Other regulations necessary to understand are *Sarbanes-Oxley (SOX) Act of 2002* (for public companies to secure the public against corporate fraud and misrepresentation) and the Gramm-Leach-Bliley (GLB) Act, which protects the privacy of consumer information held by financial institutions. Also see "monitor compliance" in the digital forensics task list later in this chapter.

3. **Security solutions development:** Design, deploy, and support the logical and physical security infrastructure for the network to safeguard intellectual property and confidential data. The starting point for the design and development can be accomplished by developing a security reference architecture that is essentially a template or blueprint to guide the security needs of the organization, including the major actors and activities. For example, the reference architecture could provide a consistent vocabulary of terms, acronyms, and definitions. This provides a common frame of reference during

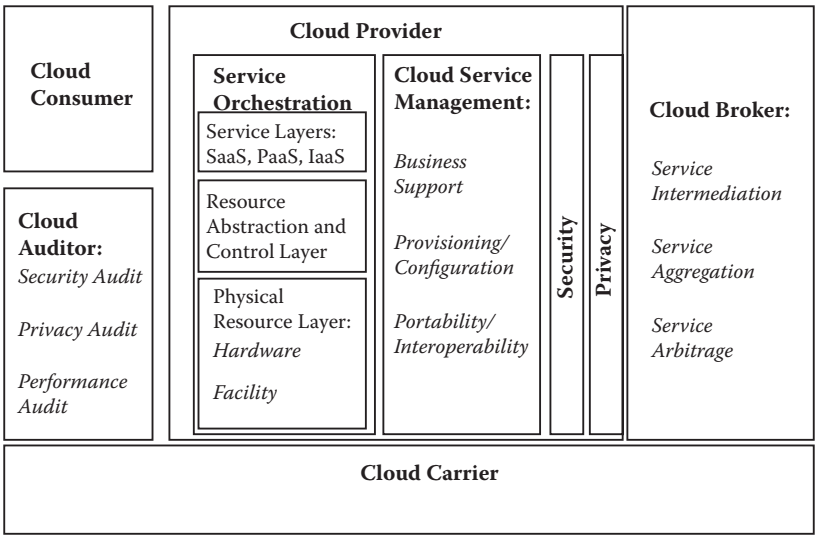



**FIGURE 2.1**
A conceptual reference model. (Modified from Liu, F. et al., 2007, NIST publication 500-292, http://www.nist.gov/customcf/get_pdf.cfm?pub_id = 909505)

communication, thus facilitating the understanding of requirements among stakeholders. Figure 2.1 shows an example of a conceptual reference model for cloud computing.

4. **Investigate the security design and features of relevant information and security products necessary to deploy the security solution:** This includes supporting technologies such as intrusion detection systems (IDS), intrusion prevention systems (IPS), security logging, public-key infrastructure (PKI), data loss prevention (DLP), firewalls, remote access, proxies, and vulnerability management.
5. **Maintain information and security products:** This task would include optimization, software upgrades, software patch installations, hardware upgrades, and diagnosis and resolution of software and hardware issues.
6. **Monitor and optimize system logs:** Review usage levels and performance; report misuse and security breaches. Provide weekly, monthly, and quarterly reports.
7. **Perform risk assessment:** This task addresses potential vulnerabilities and anticipates threats. The vulnerability assessment may be accomplished via a penetration test (aka pen-test) and/or a security audit. A pen-test is a way of testing the security of your system by simulating an attack. A security audit includes looking at all assets such as laptops, printers, routers, etc. and performing, for example, vulnerability scans

to assess the system for patch levels, open ports, etc. This essentially includes any activities that help determine whether the current configuration effectively mitigates security risks. Also see "perform risk assessment" of the computer forensics task list later.

8. **Maintain security incident handling process/plans:** This overlaps with the computer forensics profession. See "manage crisis/incident response" of the computer forensics task list later.
9. **Conduct or be involved in the incident response activities:** Be a member of the incident response team and assist in an incident investigation.
10. **Facilitate security awareness and training:** Training is important to educate and drive the implementation and standardization of the company's security program.
11. **Create and maintain the business continuity (BC) and disaster recovery (DR) plans:** In the event of a disruption to your business due to anything from a malfunctioning system upgrade to an earthquake, your DR plan will describe the process by which your company can resume business activities after this planned or unplanned downtime. The BC plan will delineate how to keep your company functioning during this downtime.

### 2.2.2 A Summarized List of "Digital Forensic" Job Tasks

1. **Participate in e-discovery cases and digital forensics investigations:** Discovery is where each party involved in a lawsuit requests information from the opposing party. This information gathered will potentially be used in a trial. When the request is for electronic information such as Word documents, spreadsheets, e-mail, audio, and video, it is referred to as e-discovery. This requires following a forensically sound process to acquire, preserve, and analyze vast amounts of data from a variety of media types in addition to monitoring the chain of custody to protect the data against alteration and damage. Reports and presentations will also need to be created for possible inclusion in legal or policy disputes. Digital forensics investigations require analysis of the data in its entirety—not just logical files. This would include log files, swap space, slack space, deleted files, etc. Further details of the digital forensic process and the differences between e-discovery and digital forensics will be covered later in the book.
2. **Perform data recovery services for users:** Not all tasks are related to criminal activity. There are times when data recovery is needed due to human error, file corruption, or when you accidentally reformat the hard drive on your video camera after your family's first trip to Disney World☺. The digital forensics professional will be able to recover data on any media including existing files, deleted yet remaining files, hidden

files, password-protected files, encrypted files, fragmented data, and corrupted data to ensure that company information is retained.

3. **Create, evaluate, and improve the effectiveness of incident response (IR) policies:** You may be working with the information security professional to maintain the security incident handling processes and plans. NIST defines the IR plan as providing the "organization with a roadmap for implementing its incident response capability" (Cichonski et al. 2012). Chapter 5 will cover incident response. NIST also recommends that the IR plan include elements that incorporate management support such as:
   a. A mission statement
   b. Strategies and goals to help determine the structure of the IR capability
   c. Senior management approval of the IR plan
   d. Determining the organizational approach to incident response
   e. Determining how the IR team will communicate with the rest of the organization
   f. Metrics for measuring the incident response capability to make sure it is fulfilling the goals
   g. Performing an annual review of the IR road map for maturing the incident response capability
   h. Determining how the IR program fits into the overall organization
4. **Manage crisis/incident response:** Respond and confirm that there is in fact a problem (knowing the signs of an incident), analyze, contain, eradicate, and recover from the incident as well as perform an after-action report to determine lessons learned.
5. **Be familiar with the legal aspects of digital forensics as well as case law:** With the ease of Internet access and acquiring computing devices, there has been an obvious increase in crimes involving digital evidence. As a result, this has increased the need for digital forensics professionals. These professionals need to be very familiar with the law (the legality surrounding acquiring digital evidence in a criminal investigation) and case law (laws based on judicial decisions given in earlier cases). For example, in the case *US v. Carey,* there was a search warrant* to search the defendant's computer for drug-related evidence. The agent discovered child pornography and continued to search the computer for child pornography evidence. That additional searching exceeded the scope of the search warrant. Therefore, that search was considered an unconstitutional

* A warrant is an order from a legal authority that allows an action such as a search, an arrest, or the seizure of property.

"general search." This restriction, based on the Fourth Amendment, which guards against unreasonable searches and seizures, caused the child pornography evidence to be suppressed from the case.

6. **Monitor the network:** This task overlaps with information security tasks. It would include the use of intrusion detection systems (IDS), intrusion prevention systems (IPS), and/or network intrusion detection (NID). In addition, creating IDS/IPS signatures (patterns of common attacks or threats) where the IDS/IPS will detect network behavior patterns that match a known attack signature may also be included in the security posture of the system. This task may also involve deep packet inspection. Packet filtering is where the data or content of a packet is inspected for threats, and it includes applying content-filtering rules, creating statistics, and routing traffic. It is important for a digital forensics professional to be included in this process or at least in configuring these systems as the data collected will help in an investigation.
7. **Perform risk assessment:** Risk assessment also overlaps with the information security professional tasks. The risk assessment will determine which threats can exploit vulnerabilities that would damage company assets. Essentially, the results of the risk assessment should help to determine or improve the company's overall security posture. In other words, the risk assessment should result in recommendations of best practices for prevention of future threats. This task may also include pen-testing, which would intend to exploit known vulnerabilities, thus confirming risk. This would also require analysis of malware, attacker tools, and even reverse engineering of threats.
8. **Monitor compliance:** Compliance does not guarantee a secure infrastructure but it may lessen the odds of a breach. In addition to what was discussed in the information security task list, the computer forensics professional also needs to understand *breach laws*. Any company storing and accessing private consumer data is required to notify its consumers when their personal information may have been breached. Due to some states varying the law, senators are attempting to pass a national law to create a single national standard (Schwartz 2012). If an agency does not "take reasonable measures to protect and secure data in electronic form containing personal information," it could face up to a $500,000 fine per incident. Table 2.1 shows six large data breaches in 2012 (Chickowski 2012).

There are two more important skills/tasks required to be successful in this field, the first of which is communication. Security is a complex topic; however, at times it needs to be explained to a nontechnical person. For example, the results of a forensic analysis may need to be communicated to a lawyer, judge, or law enforcement official who may not have a technical background and who may need to merge your analysis results with

**TABLE 2.1**

Six Big Data Breaches of 2012

| Company | Number of Records | How? |
|---|---|---|
| 1. Zappos | 24 million | Access obtained through internal network |
| 2. University of North Carolina | 350,000 | Systems misconfigurations caused back-end university systems to be exposed |
| 3. Global Payment Systems | 7 million consumer records including 1.5 million credit cards | Records exported from its North American processing system; cause unclear |
| 4. South Carolina Health and Human Services | 228,435 | An employee e-mailed himself patient records |
| 5. University of Nebraska | 654,000 | Cause of intrusion into a consolidated database was unclear |
| 6. LinkedIn | 6.5 million | Encryption scheme for passwords was cracked |

the nontechnical aspects of a case. The point is to know your audience. For example, if you are presenting a forensics analysis to the CEO, you do not need to explain the log files. An overview of what the log files showed would suffice.

The second skill/task is project management. Every upgrade, implementation, and investigation is a project, which requires managing people, time, and probably a budget. You do not need a PMP (project management professional) credential, but it would be beneficial to take a course or read a book in the area of project management.

There are an abundance of opportunities for training in the fields of cyber security and digital forensics to obtain knowledge to perform the tasks discussed here. For example, some colleges and universities are offering associate, bachelor, and graduate degrees in these professions. If you already have a degree in another area, a faster (and less expensive) way to break into this field is to earn a certification. Many training courses offered by professional or training organizations to help prepare for the certifications are outlined in the next section.

## 2.3 Certifications

Certifications are beneficial in that they give a person credibility in a particular area, can show one's commitment, create a differentiation from other job candidates, and increase earning potential. In addition, many positions

in government and corporations require certification because they need qualified personnel with the knowledge and skill set to design, implement, monitor, and protect their critical assets.

One major challenge is determining which certification to earn. Sorting through the vast amount of certifications can be just as overwhelming as the job search. Consequently, before choosing a certification to acquire, it would make sense to do a job search to see what type of certification is required for the positions that are of interest to you. It also helps to determine which certifications are the most wanted by employers. Once you figure out a few certifications that are applicable or required for the jobs of interest, you need to figure out which certification fits your needs. For example, some certifications require "recertification," some require work experience, and all vary in terms of training for the exams. Interestingly, in many of those job postings on LinkedIn and Monster.com, many certifications are listed together, for example: "CISSP [certified information systems security professional] and/or CISA [certified information systems auditor], CISM [certified information security manager], GIAC [global information assurance certification]." Some of the knowledge domains required of these certifications overlap and the employers will often substitute one certification for the other. They are not expecting you to have them all.

> A group of researchers studied job postings on Monster.com in 2009 and found that 1,249 jobs required the CISSP, 1,117 required the CISA, and 288 required the CISM (J. Nelson, D. Nelson, and N. Nelson 2009). My quick search on LinkedIn in 2012 resulted in 897 jobs requiring the CISSP, 681 requiring CISA, 356 requiring the CISM, and 158 requiring the GIAC certification (similar results in using Monster.com in 2012).

All of the most prevalent certifications are covered in this section, but not in any particular order. Similar to the job tasks presented earlier, the certifications have also been categorized in two groups: information systems security certifications (some of these cover digital forensics knowledge) and those that are strictly computer forensic certifications.

### 2.3.1 Information Security Certifications

The first set of certifications presented in this section are granted from the International Information Systems Security Certification Consortium or ISC.[2] The ISC is a well-known organization that certifies and credentials information security professionals. It offers several security certifications. Following is a brief description of the certifications. For further details, please see the ISC[2] website (https://www.isc2.org/):

- **Systems security certified practitioner (SSCP):**
  - *Work experience:* The applicant needs one year of work experience in one of the following domains: access controls; cryptography; malicious code and activity; monitoring and analysis; networks and communications; risk, response, and recovery; or security operations and administration.
  - *Knowledge domains:*
    - Access controls: Define the operations users allowed to perform on the company systems.
    - Security operations and administration: Identify information assets and guidelines to ensure information confidentiality, integrity, and availability.
    - Monitoring and analysis: Collect information for identifying and responding to security breaches.
    - Risk, response, and recovery: Conduct the process in response to an incident.
    - Cryptography: Use techniques to ensure the integrity, confidentiality, authenticity, nonrepudiation, and recovery of encrypted information in its original form.
    - Networks and communications: Implement measures to operate both private and public communication networks.
    - Malicious code and activity: Implement prevention techniques for malicious activity.
  - *Examination:* Take an in-classroom or online course before taking the exam.
  - *Endorse the certification:* Once the exam is passed, the applicant needs to have the certificate signed by a credentialed professional in good standing who can attest to the applicant's work experience.
  - *Maintain the certification:* Recertification is required every three years. This can be obtained by earning 60 credits of continuing professional education (CPE), where at least 10 credits must be completed each of the three years. There is also a yearly maintenance fee.
  - *Concentrations:* None.
- **Certified authorization professional (CAP):**
  - *Work experience:* Two years of work experience in one or more of the knowledge domains. Applicants should also have the following knowledge or skill set: IT security, information assurance, information risk management, systems administration, information security policy, technical auditing experience within government departments, and NIST documentation.

- *Knowledge domains:*
  - Understand the security authorization of information systems: Evaluate risk across the enterprise by applying a risk management framework (RMF), revising the organizational structure, and assessing the security controls.
  - Categorize information systems: The information systems are categorized to develop the security plan, select security controls, and determine risk. It is based on information included, requirements for the information, and impact on the organization if compromised.
  - Establish the security control baseline: The specific controls required to protect the system are based on the categorization, risk, and local parameters.
  - Apply security controls: Employ and test the specified security controls in the security plan.
  - Assess security controls: Determine effectiveness of the controls meeting the security requirements.
  - Authorize information systems: Evaluate risks and determine if the system should be authorized to operate.
  - Monitor security controls: Perform continuous monitoring according to the strategy specified by the organization.
- *Examination:* Take an in-classroom or online course prior to the exam.
- *Endorse the certification:* Once the exam is passed, the applicant needs to have the certificate signed by a credentialed professional in good standing who can attest to the applicant's work experience.
- *Maintain the certification:* Recertification is required every three years and is obtained by earning 60 credits of CPE and at least 10 credits must be completed each of the three years. A yearly maintenance fee is also required.
- *Concentrations:* None

- **Certified secure software life cycle professional (CSSLP):**
  - *Work experience:* Four years of experience being involved in the software development life cycle in one of the knowledge domains (following) or three years of work experience with a related college degree.
  - *Knowledge domains:*
    - Secure software concepts: Know and understand the concepts to consider when designing secure software.
    - Secure software requirements: Have effective requirement elicitation and understanding security needs from stakeholders.

  - Secure software design: Design secure software architecture and conduct threat modeling.
  - Secure software implementation/coding: Utilize secure coding practices to mitigate vulnerabilities and review code to ensure there are no errors in the code and security controls.
  - Secure software testing: Integrate software testing to test the security functionality and resiliency to an intrusion as well as how well the software can recover from an attack.
  - Software acceptance: Determine if software is free from vulnerabilities in all areas (procurement/supply chain, configuration, compliance, licensing, intellectual property, and accreditation).
  - Software deployment, operations, maintenance and disposal: Deal with security issues surrounding the steady-state operations of the software as well as any security issues surrounding the elimination of the software.
- *Examination:* Prior to the exam, students participate in webcasts, read the textbook, and attend either an online or classroom education program.
- *Endorse the certification:* Once the exam is passed, the applicant needs to have the certificate signed by a credentialed professional in good standing who can attest to the applicant's work experience.
- *Maintain the certification:* Recertification is required every three years and is obtained by earning 90 credits of CPE, and at least 15 of the credits must be completed each of the three years in addition to a required yearly maintenance fee.
- *Concentrations:* None

- **Certified information systems security professional (CISSP):**
  - *Work experience:* Five years of experience in information security. Specifically, the experience can be in two or more of the following areas: access control, telecommunications and network security, information security governance and risk management, software development security, cryptography, security architecture and design, operations security, business continuity and disaster recovery planning, compliance, and physical security.
  - *Knowledge domains:*
    - Access control: The concepts, methods, and techniques to develop a secure and effective architecture to protect assets against threats
    - Telecommunications and network security: Network concepts such as structures, transmission methods, transport formats, and security measures to protect networks, facilitate business goals, and protect against threats

  - Information security governance and risk management: Developing policies, standards, guidelines, and procedures; determining information assets and understanding risk management tools and practices.
  - Software development security: Effective application-based security controls and software development life cycle
  - Cryptography: Concepts and algorithms to disguise information and ensure its integrity, confidentiality, and authenticity
  - Security architecture and design: System and enterprise architecture concepts, principles, and benefits as well as principles of security models
  - Operations security: Control management, resource protection, vulnerability assessment, attack prevention, and incident response
  - Business continuity and disaster recovery planning: Creating response and recovery plans as well as conducting restoration activities
  - Legal, regulations, investigations, and compliance: Investigating incidents by acquiring and analyzing evidence in compliance with the law and regulations
  - Physical (environmental) security: Addressing the security of the facility both internally and at the perimeter and having layered physical defense and entry points
- *Examination:* Take an in-classroom or online course prior to the exam.
- *Endorse the certification:* Once the exam is passed, the applicant needs to have the certificate signed by a credentialed, professional in good standing who can attest to the applicant's work experience.
- *Maintain the certification:* Recertification is required every three years and is obtained by earning 120 credits of CPE education, where at least 20 credits must be completed each of the three years. A yearly maintenance fee is also required.
- *Concentrations:*
  - Architecture (CISSP-ISSAP):
    - Requirements: CISSP credential and two years of experience in systems architecture
    - Knowledge domains: Access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology-related business continuity planning, disaster recovery planning, and physical security considerations

  - Engineering (CISSP-ISSEP):
    - Requirements: CISSP credential and two years of engineering experience
    - Knowledge domains: Systems security engineering, certification and accreditation, technical management, and US government information assurance governance
  - Management (CISSP-ISSMP):
    - Requirements: CISSP credential and two years of professional management experience
- Knowledge domains: Security management practices, systems development security, security compliance management, business continuity planning, disaster recovery planning and law, investigations, forensics, and ethics

This next set of certifications is offered by the global information assurance certification (GIAC), which is a SANS (SysAdmin Audit Network Security) Institute affiliate. They offer many certificates in the following categories: security administration, forensics, management audit, software security, legal, and security expert. Following is a brief description of some of the security-based certifications offered by the GIAC. For further information, please see the GIAC website (https://www.giac.org/):

- **Security essentials (GSEC):** This certification is earned based on the knowledge of over sixty objectives. The objectives demonstrate the security tasks that are required of a professional in an IT systems hands-on role (e.g., access control, business continuity planning/disaster recovery, firewalls, honeypots, and incident handling fundamentals).
- **Certified incident handler (GCIH):** This certification is earned based on the knowledge of twenty five objectives that facilitate the management of security incidents. Specifically, the focus of this certification is on detecting, responding to, and resolving computer security incidents.
- **Certified intrusion analyst (GCIA):** This certification is earned based on the knowledge of configuring, monitoring, and analyzing the network traffic from an intrusion detection system.
- **Penetration tester (GPEN):** This certification is earned based on the knowledge of finding security vulnerabilities in a network.
- **Certified firewall analyst (GCFW):** This certification is earned based on the knowledge of designing, configuring, and monitoring routers, firewalls, and perimeter defense systems.
- **Web application penetration tester (GWAPT):** This certification is earned based on the knowledge of web application exploits and penetration testing methodology.

- **Certified Windows security administrator (GCWN):** This certification is earned based on the knowledge of securing Windows clients and servers.
- **Assessing and auditing wireless networks (GAWN):** This certification is earned based on the knowledge of security mechanisms for wireless networks as well as how to utilize the tools and techniques necessary to evaluate and exploit the vulnerabilities of a wireless network.
- **Certified UNIX security administrator (GCUX):** This certification is earned based on the knowledge of securing and auditing UNIX and Linux systems.
- **Information security fundamentals (GISF):** This certification is earned based on the knowledge of ten objectives that focus on understanding threats and risks to the company's information assets as well as the best practices to protect them.
- **Certified enterprise defender (GCED):** This certification extends the knowledge and skills of the GSEC certification such as defensive network infrastructure, packet analysis, penetration testing, incident handling, and malware removal.
- **Exploit researcher and advanced penetration tester (GXPN):** This certification is earned based on the knowledge of eighteen objectives that focus on finding vulnerabilities of target networks, systems, and applications.
- **GIAC security expert (GSE):** This certification requires having earned the GSEC, GCIH, GCIA certifications as well as having "gold" status (a paper accepted into the SANS reading room) in two of them. There are also options to substitute other GIAC certifications (details on their website). In addition to the prerequisites, this certification is earned based on the knowledge of five knowledge domains: IDS and traffic analysis, incident handling, IT SEC, security technologies, and necessary soft skills.

Each GIAC certification requires passing a proctored exam. The exams vary in length and minimum passing score. Unlike the other GIAC certifications presented here, the GSE also requires the candidate to sit for a hands-on lab. Although SANS training is available, none of the certifications require any specific training. The knowledge tested can be acquired via practical experience or by reading information security publications. All GIAC certifications are valid for four years. With the exception of the GSE certification, there are many options for recertification, such as taking the current version of the exam or taking related courses and publishing technical research. The GSE can only be maintained by passing the current version of the exam.

The third set of certifications is offered by the Sherwood Applied Business Security Architecture (SABSA) Organization. There are three distinct levels of

certification indicating the stages of proficiency from knowledge and understanding of the concepts to demonstrating and applying the subject matter in order to master the profession. The practitioner (level 2) and master (level 3) levels have prerequisites of the preceding levels. Following is a brief description of the certifications; please see http://www.sabsa-institute.org for further details:

- **SABSA chartered foundation (SCF) certificate:** The foundation certificate tests competency in two areas: *strategy and planning* and *security service management.* The testing consists of two multiple-choice exams. Training can be acquired from the SABSA textbook or from one of its training courses.
- **SABSA chartered practitioner (SCP) certificate:** This certificate requires the SCF certificate and passing two additional test modules. The topics of the two additional test modules depend on which of the four specialties are chosen:
  1. Risk management and governance (SCPR) certificate: Focus on *information assurance* and *operational risk management*
  2. Business continuity and crisis management (SCPC) certificate: Focus on *information assurance* and *business continuity management.*
  3. Security architecture design and development (SCPA) certificate: Focus on *identity and access management architecture* and *network security architecture and design.*
  4. Security operations and service management (SCPO) certificate: Focus on *identity and access management architecture* and *intrusion and incident management.*
- **SABSA chartered master (SCM) certificate:** This certificate requires the SCF, SCP, and three additional test modules. The topics of the two additional test modules depend on which of the four specialties are chosen:
  1. Risk management and governance (SCMR) certificate: Focus on *management skills, measurement and performance management,* and *information security governance*
  2. Business continuity and crisis management (SCMC) certificate: Focus *on management skills, measurement and performance management,* and *crisis management*
  3. Security architecture design and development (SCMA) certificate: Focus on *management skills, cryptographic techniques,* and *application and web security architecture and design*
  4. Security operations and service management (SCMO) certificate: Focus on *management skills, cryptographic techniques,* and *digital forensics and investigations*

The International Council of E-Commerce Consultants (EC-Council) offers another set of certifications. Similar to some of the other organizations,

the EC-Council certifies the information security professional as well as the digital forensics professional. Following is a brief description of the information security certifications:

- **Certified ethical hacker (CEH):** This certification covers how to determine the weaknesses and vulnerabilities of a computer system using the tools and skills of a malicious hacker—keeping within the law, of course. The certification also includes the knowledge to prevent and correct vulnerabilities. To be eligible for the certification exam, one can either attend official training or show at least two years of information security experience. The website provides an outline of the specific knowledge that will be tested as well as its weight on the exam. The certification is valid for three years and can be renewed with EC-Council continuing education credits.
- **EC-Council certified security analyst (ECSA):** This is essentially an advanced ethical hacking certification. There is a deeper focus on the analytical phase of ethical hacking, such as being able to analyze the outcome of hacking tools and technologies. With these skills one can perform the assessments required to identify and mitigate security risks. To earn this certification, one needs to pass a fifty-question exam.
- **Licensed penetration testing (LPT):** This certification covers the process of testing the network perimeter defense mechanisms. There are no exams. The candidate needs to have achieved the CEH and the ECSA certifications, as well as be in good standing and not have any criminal convictions.
- **EC-Council network security administrator (ENSA):** This certification tests the skills to analyze the internal and external security threats against the network. Domain knowledge for this certification include: evaluating the network, evaluating the Internet security issues and design, implementing security policies and firewall strategies, and evaluating vulnerabilities and being able to defend against them. To earn this certification, one needs to pass a fifty-question exam.

The Information Systems Audit and Control Association (ISACA) offers the final set of information security certifications covered in this book. It offers four certifications with the knowledge/task domains outlined next. For further details and information, please see their website, http://www.isaca.org:

- **Certified information security manager (CISM):**
  - *Information security governance:* Being able to develop and maintain an information security governance framework to ensure that the security strategy of the organization meets

the organization's goals and objectives, as well as managing risk and program resources
    - *Information risk management and compliance:* Managing risk in order to meet business and compliance requirements of the organization
    - *Information security program development and management:* Developing and maintaining an information security program that aligns with the organization's security strategy
    - *Information security incident management:* Assuring the ability to plan, establish, and manage the detection of, investigation of, and response to information security incidents.
- **Certified information systems auditor (CISA):** The focus of this certification is based on job tasks and practice. The tasks and knowledge needed for each of the following domains is detailed on their website:
    - *The process of auditing information systems:* Protecting and controlling information systems with IT audit practices
    - *Governance and management of IT:* Ensuring that leadership, organizational structure, and processes are able to achieve the organization's objectives and strategies
    - *Information systems acquisition, development, and implementation:* Meeting the organization's strategies and objectives when acquiring, developing, testing, and implementing the information systems
    - *Information systems operation maintenance and support:* Meeting the organization's strategies and objectives when operating, maintaining, and supporting the information systems
    - *Protection of information assets:* Ensuring that the organization's security policies, standards, and procedures protect the confidentiality, integrity, and availability of the information assets
- **Certified in the governance of enterprise IT (CGEIT):**
    - *IT governance framework:* Design, develop, and maintain an IT governance framework that includes leadership and organizational structures and processes. The framework must align with the company's governance, implement good practices to control the information and technology, and ensure compliance.
    - *Strategic alignment:* Ensure that IT supports the following: integrating IT strategic plans with business strategic plans and continuing to achieve business objectives and optimizing business processes by aligning IT services with businesses operations.
    - *Value delivery:* Ensure that IT and the business fulfill their value management responsibilities (IT services and assets contribute to the value of the business).

- *Risk management:* Ensure that the framework exists to manage and monitor IT business risks.
- *Resource management:* Ensure that the competence and capabilities of IT resources can meet the demands of the business.
- *Performance measurement:* Set, monitor, and evaluate business-supporting IT goals.

- **Certified in risk and information systems control (CRISC):**
  - *Risk identification, assessment, and evaluation:* Execute the enterprise risk management strategy.
  - *Risk response:* Develop and implement risk responses to address risk factors and incidents.
  - *Risk monitoring:* Communicate risk indicators to stakeholders.
  - *Information systems control design and implementation:* Design and implement information system controls.
  - *IS control monitoring and maintenance:* Effectively monitor and maintain the information systems controls.

### 2.3.2 Digital Forensic Certifications

Like the information security certifications, there are many digital forensic certifications. Some are offered by product vendors, some by professional organizations, and some by training providers. Until there are more degrees offered in this field, it would be safe to say that with this highly specialized profession, a certification is most likely a must. Following are some of the vendor-neutral certifications.

#### *2.3.2.1 Global Information Assurance Certifications*

In the previous section we covered the security-based certifications offered by the GIAC. Next we will present a brief description of some of the forensics-based certifications offered by the GIAC. For further information, please see the GIAC website (https://www.giac.org/):

- **Certified forensic analyst (GCFA):** The focus of this certification is on the skills and knowledge necessary to collect and analyze data from digital media. One can prepare for the proctored exam by taking the SANS training course, Advanced Computer Forensic Analysis and Incident Response. This certification must be renewed every four years by either taking the exam again or earning 36 certification maintenance units (CMUs). The CMUs range from attending more training to publishing a related paper or book.
- **Reverse engineering malware (GREM):** This certification tests the knowledge and skills one needs to protect an organization from

malicious code by reverse-engineering malware. One can prepare for the proctored exam by taking the SANS training course, Reverse-Engineering Malware: Malware Analysis Tools and Techniques. This certification must be renewed every four years by either taking the exam again or earning thirty-six CMUs. The CMUs range from attending more training to publishing a related paper or book.

- **Certified forensic examiner (GCFE):** The candidate with the GCFE will be able to conduct investigations that include e-discovery, forensic analysis and reporting, evidence acquisition, browser forensics, and tracing user and application activities. One can prepare for the proctored exam by taking the SANS training course, Computer Forensic Investigations—Windows In-Depth. This certification must be renewed every four years by either taking the exam again or earning 36 CMUs. The CMUs range from attending more training to publishing a related paper or book.
- **Certified computer examiner (CCE):** The next certification is the CCE, which is the primary certification offered by the International Society of Forensic Computer Examiners (ISFCE). ISFCE is a private organization that offers training and certification. The CCE also performs research and development into new technologies and methods for computer forensics (http://isfce.com/). This certification includes a practical exam as well as an online written exam. A candidate who passes the online exam will have ninety days to complete the practical exam. Recertification consists of forty CPE credits and practice in the field, which needs to occur after two years.
- **Certified forensic computer examiner (CFCE):** The International Association of Computer Investigative Specialists (IACIS), a nonprofit organization that trains computer forensics professionals, offers a two-week course designed to prepare candidates for the CFCE. The training course is not required to enter into the CFCE certification process. The CFCE process consists of completing a series of practical exercises. Upon successful completion of these exercises, the candidate needs to pass a comprehensive written exam. The knowledge domains covered are as follows: preexamination procedures and legal issues, media examination and analysis, data recovery, specific analysis of recovered data, reporting and exhibits, and defense and presentation of findings. The CFCE requires a recertification every three years that includes an exam and 60 hours of continuing education in the field. For further details, please see http://www.iacis.com.
- **Computer hacking forensic investigator (CHFI):** As mentioned in the previous section, the EC-Council also offers a computer forensic certification. This certification focuses on the process of detecting hacking attacks and properly extracting evidence to report crimes,

conduct audits, and prevent future attacks. The candidate is awarded the certification upon successful completion of the 150-question exam. Further details can be found on the EC-Council website (https://cert.eccouncil.org/).

- **Professional certified investigator (PCI):** ASIS International offers the professional certified investigator. This certification is awarded upon successful completion of a multiple-choice exam covering case management, investigative techniques and procedures, and case presentation. The PCI has a three-year recertification term that can be accomplished with 45 CPE credits.
- **Certified computer forensics examiner (CCFE):** The Information Assurance Certification Review Board (IACRB) offers the CCFE. This certification tests a candidate's knowledge of the following knowledge domains: law and ethics, investigation process, computer forensic tools, device and evidence recovery and integrity, file system forensics, evidence analysis and correlation, evidence recovery, and report writing. The CCFE requires a fifty-question multiple-choice exam and a practical exam (given upon successful completion of the multiple choice exam). The IACRB is a professional nonprofit organization whose sole mission is to certify individuals. One can get training for the exam from an IACRB-approved training provider. Please see http://www.iacertification.org/for further information.

#### *2.3.2.2 Software Certifications*

In addition to the vendor-neutral certifications, two well-known forensic software packages offer certifications: EnCase (ENCE) and AccessData Certified Examiner (ACE). These certifications appear in many job postings (along with other certifications, of course); therefore, it was added to this listing of certifications.

Guidance Software's EnCase is a one of the industry-standard computer investigation tools. It essentially enables the investigator to acquire the data and evidence from many devices to create reports and maintain the integrity of the evidence. The **EnCE** is the EnCase certification offered by Guidance Software that ensures the mastery of the computer investigation methodology as well as effective use of the EnCase software during an investigation. This certification requires 64 hours of computer forensic training or one year of computer forensic work experience, the approval of the EnCE application, passing the written exam, and passing the practical exam. The candidate has sixty days to complete the practical exam. The certification renewal has a few options, but essentially requires 32 hours of training every three years. For further information, see *www.guidancesoftware.com.*

Another industry-standard computer forensics software package is AccessData Group's **Forensic Toolkit (FTK).** FTK is similar to EnCase in that

it is used in investigations to image, analyze, and report. The AccessData certified examiner (ACE) demonstrates proficiency with FTK. The certification consists of one multiple-choice exam. The candidates need to have access to a computer with a licensed version of FTK, since the questions relate to analyzing an image in FTK by the candidate. One year after passing the ACE exam, the candidate is required to pass an online practical examination. After the practical exam, the certification needs to be renewed every two years. There are free online videos to prepare for the exam. For further information, see www.accessdata.com.

Computer Analysis Response Team

If you have any aspirations to work for the US government, there are opportunities at the many different government agencies as most have a computer forensic need. The four main FBI priorities that require computer forensic support are *innocent images* (a program that identifies pedophiles who use the Internet to lure children or spread child pornography), *counterintelligence* (combating the infiltration of the US intelligence community by foreign intelligence services), *counterterrorism* (addresses terrorist threats), and *criminal* (white collar crimes such as fraud and public corruption). Each FBI field office has a computer forensic unit called the Computer Analysis Response Team (CART) whose primary function is to retrieve evidence from electronic media. CART training, available for both agents and professional support within the Bureau, includes some of the industry certification exams discussed in this chapter. For more information, please see www.fbi.gov.

## References

Chickowski, E. 2012. 6 Biggest breaches of 2012 so far. *Dark Reading,* June 20, 2012, http://www.darkreading.com/insider-threat/167801100/security/news/240002408/6-biggest-breaches-of-2012-so-far.html?itc=edit_stub (retrieved July 18, 2012).

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. Computer security incident handling guide. NIST special publication 800-61, revision 2, August 2012.

Eckelberry, A., Dardick, G., Folkerts, J., Shipp, A., Sites, E., Steward, J., and Stuart, R. 2007. Technical review of the trial testimony State of *Connecticut v. Julie Amero.* http://www.sunbelt-software.com/ihs/alex/julieamerosummary.pdf (retrieved May 18, 2012).

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D. 2007. NIST cloud computing reference architecture: Recommendations of the National Institute of Standards and Technology. NIST publication 500-292, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 (retrieved July 18, 2012).

Nelson, J., Nelson, D., and Nelson, N. 2009. Information security employment: An empirical study. *Proceedings of the 10th WSEAS International Conference on Mathematics and Computers in Business and Economics,* pp. 297–300.

SANS. n.d. InfoSec acceptable use policy. http://www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf (retrieved July 18, 2012).

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., and Steinberg, D. 2008. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. NIST special publication 800-66, http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (retrieved July 18, 2012).

Schwartz, M. 2012. Senators float national data breach law, take four. *Information Week,* June 25, 2012.

# 3

# *Cyber Security*

> Distrust and caution are the parents of security.
>
> **—Benjamin Franklin**

## 3.1 Introduction

And the winner is…Heartland Payment Systems for the single largest data breach in US history. Heartland is a business that provides payment transactions, which means it acts as an intermediary between merchants and the banks and clearly has a significant amount of personal customer data stored on its systems. The data that were stolen, as I am sure you have already guessed, were payment card data (130 million credit card numbers, expiration dates, and cardholder names). The Heartland Payment System's hacker, who also is responsible for the TJX breach in 2007, used an SQL (structured query language) injection that exploited the vulnerabilities in the database layer of the company's website with simple database commands. SQL injections are unfortunately not uncommon and have been part of other data breaches. Table 3.1 shows some other large data breaches.

The scariest part of this data breach is that Heartland was fully compliant with the Payment Card Industry Data Security Standard (PCI-DSS) at the time of the intrusion. The takeaway from this incident is that "compliance with industry standards is no guarantee of security" (Vijayan 2010). Thus, the need to go beyond the standards is a must. It is a wake-up call for companies that feel they are secure by passing the PCI security audit. This is not to say that PCI and other standards are not good, but rather is simply pointing out that companies need to monitor their assets and points of entry continuously. For example, companies need to realize that they need to protect not only the most critical servers but also the servers that control things such as heating, venting, and air conditioning—"the ones that seem less important," said Peter Tippett, vice president of technology and innovation at Verizon Business (King 2009). If you ask a hacker, he or she will tell you that those "noncritical," possibly forgotten servers are the ticket inside your network. In sum, risk assessment needs to be proactive and continuous because the threats are continuously changing.

**TABLE 3.1**

Large Data Breaches

| | | |
|---|---|---|
| Global Payments | January 2012 | 1.5 Million accounts |
| CardSystems Solutions | January 2005 | 40 Million accounts |
| TJX Companies | January 2007 | 90 Million accounts |

Whether you are a manager that needs to establish and implement an information security program or an engineer that wants to understand the information security program where you work, this chapter is a great place to start, as it is an overview of the major components that are recommended to be part of any security program. First, let us define two terms: information security and cyber security. *Information security* is the process of protecting data against unauthorized access while ensuring its availability, privacy, and integrity. *Cyber security* is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access; in other words, it implies more than the protection of data. Therefore, information security can really be considered a subset of cyber security. However, in reality, these terms are used interchangeably. We can conclude that the difference between information security and cyber security is that cyber security includes a few additional elements such as application security, network security, disaster recovery, and business continuity planning. Just in case there are any linguists reading this chapter, the history of the word "cyber" was explained by Ed Felten in his 2008 article, "What's the Cyber in Cyber-Security?" Essentially, it started with a Greek word that implies a boat operator; then Plato used it to mean "governance," and then, in the twentieth century, Norbert Wiener used "cybernetics" to refer to the robot controller. Finally, William Gibson in his novels about the future coined the word "cyberspace." Now it seems that the word "cyber" is put in front of anything and everything associated with the Internet.

## 3.2 Information Security

Information security is a system consisting of many parts: software, hardware, data, people, procedures, and networks (Whitman and Mattord 2012). Each component of the system clearly has different security requirements, but they are all based on the CIA Security Triad Model (44 United States Code, Section 3542). The following are the official definitions of the security characteristics as well as the model (Figure 3.1):

*Availability:* Ensuring reliable **access to** and **use of** information at all times

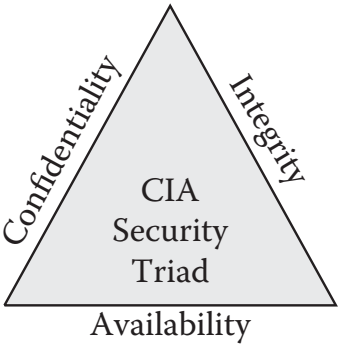



**FIGURE 3.1**
Security triad.

*Confidentiality:* Preserving authorized **restrictions on access and disclosure**, including means for protecting personal privacy and proprietary information

*Integrity:* Guarding against improper information modification or destruction, and **ensuring information nonrepudiation** (nondenial or proof of something) **and authenticity**

To ensure that these characteristics are integrated into a plan to secure the critical assets of the enterprise, the information security professional needs continuously to assess everything and anything that would affect the integrity, availability, and confidentially of the information (e.g., unauthorized access, destruction, modification, natural disasters, power failure, etc.) because, as we mentioned, the threats and technology keep changing.

This is clearly a massive topic that has been covered in many books and articles. The goal of this chapter is not to turn someone into an information or cyber security professional but rather to provide a foundation to understand the main topics of information and cyber security. Let us begin with the established information, concepts, and activities that make up information security—in other words, what is the common body of knowledge (CBK) for information security is.

Researchers Theoharidou and Gritzalis (2007) created a classification scheme outlining the ten basic domains for the information security profession based on their review and analysis of curricula, courses, university programs, and industry needs.

1. Security architectures and models
2. Access control systems and methodologies
3. Cryptography
4. Network and telecommunications and security
5. Operating system security

**TABLE 3.2**

Information Security CBK

| CISSP Domains | Theoharidou Domains |
|---|---|
| Access control | Access control systems and methodologies |
| Telecommunications and network security | Network and telecommunications security |
| Software development security | Program and application security |
| Cryptography | Cryptography |
| Security architecture and design | Security architecture and models |
| Business continuity and disaster recovery | Business and management of information systems security |
| Legal, regulations, investigations, and compliance | Social, ethical, and legal consideration |
| Physical (environmental) security | Physical security and critical infrastructure protection |
| Information security governance and risk management | |
| | Operating systems security |
| Operations security | |
| | Database security |

6. Program and application security
7. Database security
8. Business and management of information system security
9. Physical security and critical infrastructure protection
10. Social, ethical, and legal consideration

Not surprisingly, most of these domains overlap with the CBK of the CISSP (certified information systems security professional) certification (Table 3.2).

The remainder of this chapter will be dedicated to an overview of each element in the information security CBK.

## 3.3 Security Architecture

Security architecture is essentially a description or plan of how the *security controls* are related to information systems. The controls are what will help maintain the triad (integrity, availability, and confidentiality). In their book, *Principles of Information Security* (2012), Whitman and Mattord describe the many elements that complete a security architecture design. A few of the components—Spheres of security, levels of control, defense in depth, and security perimeter—will be summarized in this section.

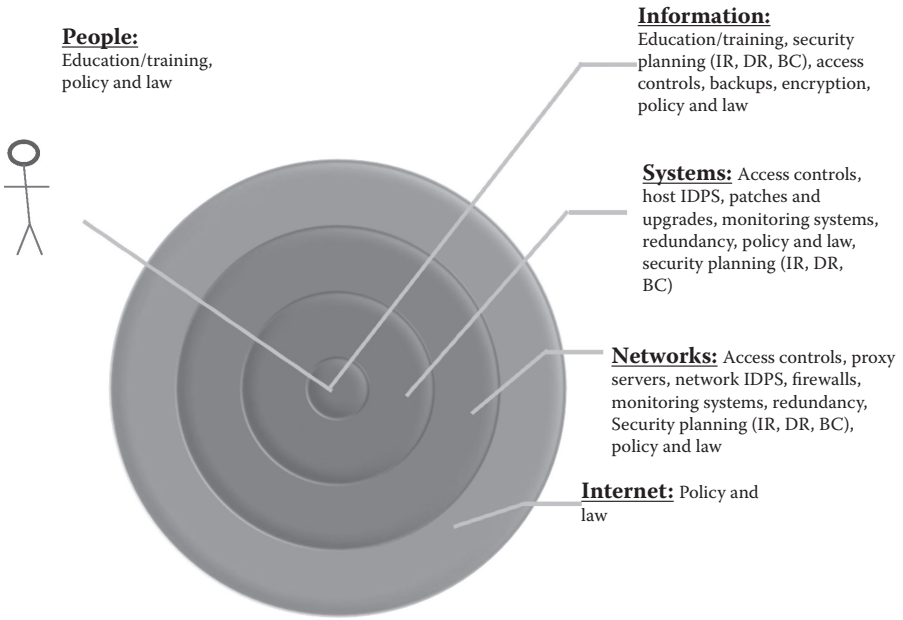



**FIGURE 3.2**
Spheres of security. (Adapted from Whitman, M., and Mattord, H., 2012, *Principles of Information Security.* Stamford, CT: Cengage Learning, Course Technology.)

A version of their *sphere of security* is shown in Figure 3.2. The sphere illustrates how information is accessed and needs to be protected. Listed next to each layer name are the protection elements. For example, "education/training" and "policy and law" are the protection between people and information. The protections between the Internet and networks are access controls, host intrusion, detection, and prevention systems (IDPS), firewalls, monitoring systems (sniffers), redundancy (implementing backup security), security planning (business continuity, disaster recovery, and incident response), and policy and law. All of these protection mechanisms will be discussed in upcoming sections.

There are three types of *levels of control:* managerial, operational, and technical. At the managerial control level, the security strategic plan is determined as well as risk management, security control reviews, and setting the guidelines to maintain any compliance required. At the operational control level, disaster recovery and incident response are planned. Also addressed at this level are personnel and physical security. The operational controls are integrated into specific business functions and the technical control level covers the components that protect the information assets.

*Defense in depth* is the layered implementation of security where the layers are policy (e.g., preparing the organization to handle attacks), training and education (e.g., defending against social engineering tactics), and technology (multilayered: firewalls, proxy servers, and access controls).

And, finally, the *security perimeter* defines the boundary between the organization's security and external entities. This is at the network level and the physical level (e.g., entrance to the building).

## 3.4 Access Controls

Access control refers to a security feature that manages the interaction with a resource. The resource can be either technology or a room containing the technology (physical security). In this section, we will focus access control with technology and discuss physical security in Section 3.11.

Access control is critical to minimizing system vulnerabilities. It restricts not only who or what has access to the resource, but also the type of access that is permitted. Here is access control explained in five "easy" steps (Gregory 2010):

1. Reliably identify the user/system
2. Find out what resource the user/system wishes to access
3. Determine if the user/system has permission to access the resource
4. Permit or deny access
5. Repeat

For an access control plan that is slightly more detailed than this one, let us refer to NIST (National Institute of Standards and Technology). They have documented security control baselines that are recommended to be employed depending on the impact level (information dependent) of the information system (low, moderate, high). In addition to access control, NIST also recommends controls for the following categories: awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personal security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Specifically, to determine the impact level of a system (low, moderate, high), the type of information processed, stored, or transmitted by or on the system needs to be determined. Once the type of information is known, the impact level of the information system can be determined by using the guidelines in the Federal Information Processing Standard (FIPS) Publication 199 (Evans, Bond, and Bement 2004). This document indicates the potential impact (level) by defining the adverse effects of a security breach that each level has on the organization's operations, assets, or individuals. For example, the impact would be defined as HIGH if the "loss of confidentiality, integrity,

or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." *Severe* is defined as the following:

1. Severe degradation in or loss of mission capability where the organization is not able to perform one or more of its primary functions
2. Major damage to organizational assets
3. Major financial loss
4. Severe harm to individuals (loss of life or life-threatening injuries)

An impact level is determined separately for the *confidentiality,* the *integrity,* and the *availability* of the information on the system. The final security category (SC) will then be determined by the highest impact level of the *confidentiality, integrity,* or *availability* of the system. An example of an SC expression of a high-impact information system is as follows:

SC = {(**confidentiality,** *low*), (**integrity,** *high*), (**availability,** *moderate*)}

For the impact to be considered *low,* all three categories need to be *low;* to be considered moderate, there must be only low and moderate levels indicated. Thus, in the preceding example, the impact level is *high* since an **integrity** loss of the information on that system was evaluated to be *high* impact. Once the SC is determined, the security controls can be selected, tailored, and supplemented if needed (Locke and Gallagher 2009).

Each security control listed in each category has an associated priority code. The priority code indicates the recommended sequencing of implementation. For example, ALL controls with the highest priority are implemented first (if that control is indicated for the system's impact level), and then implementation of the controls in the next priority level would be implemented, and so on.

The control baselines for each impact level are listed in the NIST special publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." Following is a simplified view of the *priority 1* recommendations for the **access control** baseline. Note that a control may be required for multiple impact levels but that level may require additional "control enhancements" (added functionality) to increase the strength of that particular control. The control enhancements are not specified in the following table:

| | Impact Level | | |
|---|---|---|---|
| **Control Name** | **Low** | **Moderate** | **High** |
| Develop, distribute, and maintain access control policy and procedures | ✓ | ✓ | ✓ |
| Manage IS user accounts | ✓ | ✓ | ✓ |

(*Continued*)

| Control Name | Impact Level | | |
|---|---|---|---|
| | Low | Moderate | High |
| Enforce access to system according to policy | ✓ | ✓ | ✓ |
| Control the information flow between and within systems | Not selected | ✓ | ✓ |
| Least privilege (allowing enough access to do one's job) | Not selected | ✓ | ✓ |
| Display privacy and security notifications to users | ✓ | ✓ | ✓ |
| Identify permitted actions without identification or authentication | ✓ | ✓ | ✓ |
| Document methods of remote access | ✓ | ✓ | ✓ |
| Establish usage restrictions and guidance for the implementation of wireless access | ✓ | ✓ | ✓ |
| Establish access control for mobile devices | ✓ | ✓ | ✓ |
| Establish the terms and conditions when using external information systems | ✓ | ✓ | ✓ |

Of course, prior to any access or the controlling of access, the system needs first to identify the user (user ID). The NIST suggests the following considerations for user identification, authentication, and passwords (Swanson and Guttman 1996).

**Identification** means to *require identification* of users and *correlate actions to users* by having the system maintain the IDs of active users and linking those users to identified authorized actions. The *maintenance of user IDs* occurs by deleting former and inactive users as well as adding new users.

**Authentication:** The system also needs to validate the identification claim. Possible means to authenticate are something the user *knows* (e.g., password, personal identification number [PIN], or cryptographic key), something the user *possesses* (e.g., smartcard or USB token), or something the user *is* (e.g., a biometric such as a fingerprint, voice recognition, iris scan, facial scan, handwriting, or voice recognition). Authentication can become tricky, however, due to the bring-your-own-device (BYOD) model. More and more companies are dealing with the use of employee-owned devices connected to the corporate network. For example, what if that device, which probably contains sensitive data or documents, is lost or stolen? One solution is the Tactivo smart casing shown in Figure 3.3. The sensitive information can only be accessed via a smartcard or fingerprint or both depending on the security policy.

The biometric has the greatest advantage since a user ID, password, and token can be more easily impersonated than the biometric (Gregory 2010). The downsides are the cost of maintaining biometric implementation, gradual or sudden changes in user characteristics, and false readings.

Other safeguards suggested by NIST for authentication are requiring users to authenticate, restricting access to authentication data, securing transmission of authentication data, limiting log-on attempts, securing authentication as it is entered (suppress display), and administering data properly (disable lost/stolen passwords or token and monitor systems looking for stolen or shared accounts).


**FIGURE 3.3**
Tactivo iPhone finger swipe and smartcard reader from PreCise Biometrics (http://www.precisebiometrics.com/).

Note that passwords should have required attributes (minimum length and special characters) and should be changed frequently. Users should also be trained not to "give it away" (e.g., easily guessed, posting it on their computer, telling a friend).

In addition to identification and authentication, access control needs to include authorization and accountability (Whitman and Mattord 2012).

**Authorization** is matching the authenticated entity to a list of access and control levels. This can be accomplished individually or as a group. An access control list (ACL) can be used. An ACL is a list of users who have been given permission to use a particular resource; in addition to the type of access they have been permitted.

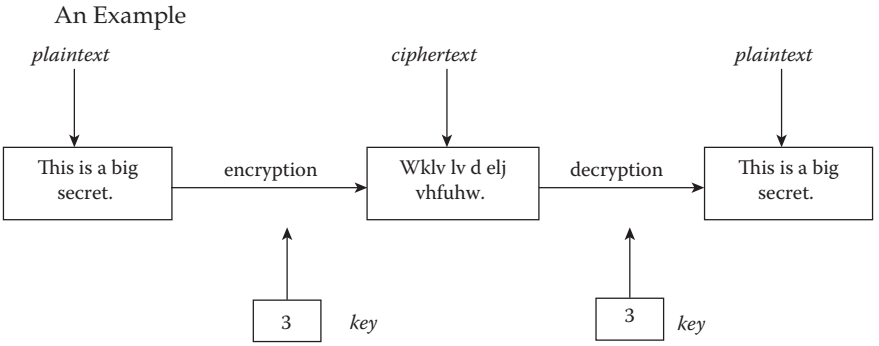
**Accountability** is using logs and journals to record the use or attempted use of a particular resource.

There are also many access control technologies. Two popular technologies are *Kerberos* and *Active Directory*. Kerberos is a network authentication protocol one can obtain from MIT (http://web.mit.edu/kerberos/). Kerberos uses strong cryptography to connect a client and server to each other and is able to assist in encrypting the communication between the two over a nonsecure network (the hosts must be trusted, however). The premise of Kerberos is that it not only prevents outside attacks, but can also minimize the attacks that occur from within the firewall. This is done by not sending passwords over the network in cleartext. Instead, it actually sends a "key" to the password. Active directory (based off the lightweight directory access protocol—LDAP) is a domain controller that maintains user account and login information. Active Directory is used by Windows to keep track of the access and security rights assigned to each user.

## 3.5 Cryptography

Cryptography is used to conceal and disguise information. Cryptography uses an encryption algorithm and a key to change data until they are unrecognizable. In other words, it uses an algorithm to scramble the data so that only a person with the proper key can unscramble them. Cryptography not only provides confidentiality and integrity of the data, but it also can provide nonrepudiation (Conrad 2011). Nonrepudiation means the authenticity of the data or information cannot be challenged.

Cryptography is not a new concept. It was used over 2000 years ago in the days of Julius Caesar for military purposes where he communicated with his troops using a shift cipher (aka Caesar cipher or substitution cipher). In a shift cipher, each plaintext letter is replaced with another letter a certain number of places further down in the alphabet. The number of places is called the *key*.




In modern times, obviously, the encryption needs to be more complex but the bottom line is that it depends on the needs of the organization and the sensitivity of the data. Here are a few, more complex cipher methods used to encrypt plaintext (Whitman and Mattord 2012):

*Transposition cipher:* The values with a block are rearranged to create the ciphertext. The rearrangement depends on the key pattern. For example, if the key pattern states:

| Text position | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Moves to position | 3 | 1 | 4 | 5 | 7 | 8 | 2 | 6 |

Use the key pattern to rearrange the plaintext to ciphertext:

| Text position | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| Plaintext | S | T | R | E | N | G | T | H |
| Ciphertext | R | E | S | N | G | H | T | T |

*Exclusive OR (XOR):* Two bits are compared. If both are the same, the result is 0. If they are different, the result is a 1. To perform the XOR cipher method, the XOR is performed on a key value with the value being encrypted—for example:

| | | |
|---|---|---|
| Plaintext | A | 01000001 |
| Key | V | 01010110 |
| Ciphertext | A XOR V | 00010111 |

*One-time pads (aka Vernam cipher):* This cipher, invented by Gilbert Vernam while he was working at AT&T, adds a random set of characters (only used one time) to a block of plaintext (of the same length). Each character of the plaintext is turned into a number and a pad value is added to it. The resulting sum is converted to ciphertext. If the sum of the two values is above 26, then 26 is subtracted from the total. Here is an example using one letter:

Plaintext = E

Plaintext value = 5

One-time pad text = J

One-time pad value = 10

Since the sum of plaintext and the pad is 15 (thus less than 26), it is converted to the ciphertext letter O.

*Book cipher:* The ciphertext contains a list of codes that represent the page number, line number, and word number of the plaintext in a particular book. The encoded message may look like this (50, 20, 5; 75, 30, 3; 300, 4, 7). Thus, on page 50, line 20, word number 5 is the first word in the message. The second word in the message is on page 75, line 30, word number 3, and so on.

### 3.5.1 Types of Cryptography or Cryptographic Algorithms

There are essentially three types of encryption: symmetric, asymmetric, and hashing (Conrad 2011):

*Symmetric key encryption:* Using the same key to encrypt and to decrypt. This encryption technique came first. The disadvantage to this type of encryption is that it is difficult to distribute the key securely. If the wrong person gets the key, you are out of luck because anyone who has the key can decrypt your message. There are many different types of symmetric encryption. The most widely known, developed by IBM, is data encryption standard (DES). The successors to DES are triple DES (3DES) and advanced encryption standard (AES). This type of encryption can be used if the two computers that are communicating are known so that the key can be installed on each computer.

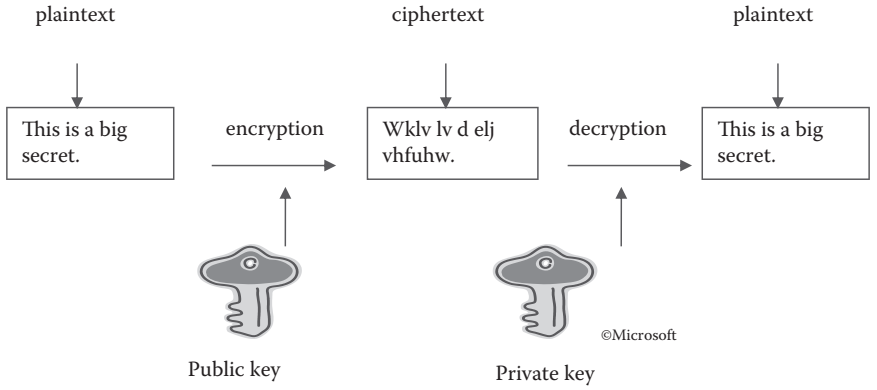



**FIGURE 3.4**
Asymmetric encryption example.

*Asymmetric key encryption:* Also known as public-key cryptography, asymmetric key encryption uses one key to encrypt and a different key to decrypt. The encryption key is a public key and anyone with a copy of the key can encrypt information that only you can read with the private key for decryption. This type of encryption solves the problem of symmetric key encryption, that the key can be easily accessed by an attacker. The private key is only known by your computer, while the public key is known by anyone who wants to communicate securely with your computer. Even if the message is intercepted in transit, you can only read it with the private key. An example can be found in Figure 3.4.

*Hash functions:* No key is used for hashing. Hash functions are mostly used to confirm data integrity (that the data have not changed). There are many hash algorithms used. One of the widely used hash algorithms is MD5. A good algorithm is determined by having a limited number (e.g., one in one billion) of collisions (two distinct files resulting with the same hash value). When the hash algorithm is performed on the plaintext, a hash value is created. Therefore, if the plaintext changes, so will the hash value.

## 3.6 Network and Telecommunications Security

The *telecommunications* and *network security* knowledge domain includes a vast amount of concepts and technology needed to protect the security triad (confidentiality, integrity, and availability). These include fundamental

network concepts such as network structures, transmission methods, and transport formats in order to provide authentication for transmissions over private and public communications networks and media. Clearly, someone working in the cyber security area would need a deep understanding of those fundamental concepts to know what he or she is protecting. However, that topic deserves its own book and thus is out of the scope of this section. The focus and goal of this section is for the reader to gain an understanding about the controls that need to be considered to secure the *networks* and to protect the *transmission* of data over a network (*telecommunications*). Following is a simplified view of the *priority 1* recommendations by NIST for the **system and information integrity** baseline:

| | Impact Level | | |
|---|---|---|---|
| **Control Name** | **Low** | **Moderate** | **High** |
| Develop system and information integrity policy and procedures that define, facilitate, and implement the roles, responsibilities, management commitment, and coordination among organizational entities and compliance | ✓ | ✓ | ✓ |
| Test, correct, and report information system flaws | ✓ | ✓ | ✓ |
| Malicious code protection at all information system entry points and any device connected to the network | ✓ | ✓ | ✓ |
| Information system monitoring to identify unauthorized use and any attacks | Not selected | ✓ | ✓ |
| Continually receive security alerts, advisories, and directives from a designated external organization | ✓ | ✓ | ✓ |
| Verify the correct operation of security functions | Not selected | Not selected | ✓ |
| The information system monitors software and information integrity | Not selected | ✓ | ✓ |
| Spam protection at all information system entry points and any device connected to the network | Not selected | ✓ | ✓ |
| The system validates information input | Not selected | ✓ | ✓ |

There are other control baselines that could also be applied to the security of network and telecommunications. It would be best to review the NIST special publication 800-53 to determine which controls would be most effective for your situation.

## 3.7 Operating System Security

The topic of operating system (OS) security overlaps with many of the topics in this chapter. The most essential security mechanism for an OS is *access control,* which was covered in Section 3.4. The OS actually facilitates the enforcement

mechanism of the access control (e.g., which users or systems can perform which operations using which resources). As mentioned previously, the type of access control is determined by the protection needed. The amount of protection is based on the system's impact level (low, moderate, high).

Jaeger (2008) describes three guarantees of a secure operating system:

1. **Complete mediation:** All security-sensitive operations are facilitated.
2. **Tamperproof:** The access enforcement cannot be modified by untrusted processes.
3. **Verifiable:** The system should be testable to demonstrate that security goals are being met.

Many companies have mail servers; hence, reviewing the NIST-recommended checklist for securing a mail server operating system is a great example of an OS security task (Tracy et al. 2007):

| Category | Action | Completed |
|---|---|---|
| *Patch and upgrade* | | ✓ |
| | Create and implement a patching process | |
| | ID, test, install patches and upgrades to OS | |
| *Remove or disable unnecessary services and applications* | | |
| | Remove or disable unnecessary services and applications | |
| | Use separate hosts for other services (web, directories, etc.) | |
| *Configure operating system user authentication* | | |
| | Remove or disable unneeded default accounts and groups | |
| | Disable noninteractive accounts | |
| | Create the user groups for the particular computer | |
| | Create the user accounts for the particular computer | |
| | Create an effective password policy (e.g., length, complexity) and set accounts appropriately | |
| | Configure computers to prevent password guessing | |
| | Strengthen authentication by installing and configuring other security mechanisms. | |
| *Configure resource controls appropriately* | | |
| | Set access controls for resources (e.g., files, directories, devices) | |

(*Continued*)

| Category | Action | Completed |
|---|---|---|
| | Limit privileges to authorized administrators for most system-related tools | |
| *Install and configure additional security controls* | | |
| | Install and configure software to provide additional controls not available in the OS | |
| *Test the security of the OS* | | |
| | Test OS after initial installation for vulnerabilities | |
| | Periodically test OS for new vulnerabilities | |

## 3.8 Software Development Security

To develop and maintain software free from security problems is no easy task. It is one of the many nonfunctional requirements a software engineer needs to design into software, (e.g., usability, maintainability, scalability, availability, extensibility, security, and portability). But, in this era, special attention needs to be paid to the security requirement. This can be achieved by building security into applications during the development process (Khan and Zulkernine 2008). However, two of the difficulties software developers face are the lack of application security knowledge and schedule pressures (Payne 2009). The eight-step process developed by Talukder et al. (2009) to elicit both functional and nonfunctional security requirements can be part of the solution where the security issues of the application are analyzed up front. Following is the summarized version of the eight steps:

1. **Functional requirements:** Capture requirements using UML analysis artifacts.
2. **Identification of assets:** Identify the critical assets of the organization and categorize them by their perceived value and loss impact.
3. **Security requirements:** Determine possibilities (diagram a misuse case; see the example in Figure 3.5) for attacks (e.g., denial of service [DOS], data tampering) and tampering with the data characteristics (e.g., confidentiality, integrity, and availability).
4. **Threat and attack tree:** Analyze each misuse case and determine the threat path.
5. **Rating of risks:** Assign values to each threat/risk to determine the highest risk.
6. **Decision on in vivo versus in vitro:** Determine which threats need to be addressed within the application (in vivo). This is done by comparing the threats to the assets.

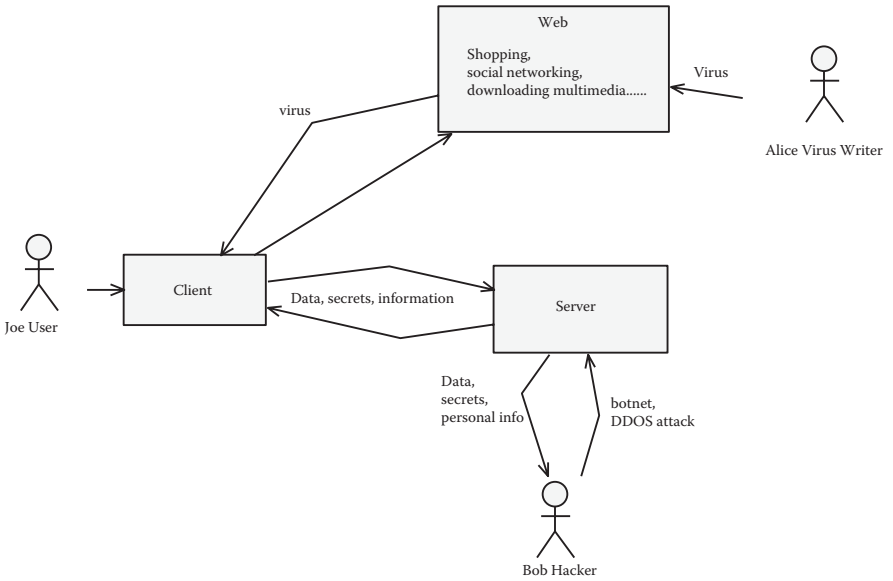



**FIGURE 3.5**
Misuse case of risk assessment.

7. **Nonfunctional to functional requirement:** Move threats that are in vivo to the functional requirements.
8. **Iterate:** Revisit and refine requirements.

No matter how diligent our software developers become in incorporating security in their software applications, we can guarantee that hackers will remain persistent in their efforts to find new ways to exploit the vulnerabilities in software. In an effort to educate software developers on common software weaknesses, the SANS Institute and the MITRE Corporation (a not-for-profit organization) collaborated with many top security experts to develop the list of the "Top 25 Most Dangerous Software Errors" (Martin et al. 2011). Over 20 organizations provided input on this list. These errors are ranked based on their evaluation of the prevalence, importance, and likelihood of each weakness. SQL injections are the top software error—which is no surprise.

| Score | ID | Name |
|---|---|---|
| 93.8 | CWE-89 | Improper neutralization of special elements used in an SQL command ("SQL injection") |
| 83.3 | CWE-78 | Improper neutralization of special elements used in an OS command ("OS command injection") |

(*Continued*)

| Score | ID | Name |
|---|---|---|
| 79.0 | CWE-120 | Buffer copy without checking size of input ("classic buffer overflow") |
| 77.7 | CWE-79 | Improper neutralization of input during web page generation ("cross-site scripting") |
| 76.9 | CWE-306 | Missing authentication for critical function |
| 76.8 | CWE-862 | Missing authorization |
| 75.0 | CWE-798 | Use of hard-coded credentials |
| 75.0 | CWE-311 | Missing encryption of sensitive data |
| 74.0 | CWE-434 | Unrestricted upload of file with dangerous type |
| 73.8 | CWE-807 | Reliance on untrusted inputs in a security decision |
| 73.1 | CWE-250 | Execution with unnecessary privileges |
| 70.1 | CWE-352 | Cross-site request forgery (CSRF) |
| 69.3 | CWE-22 | Improper limitation of a pathname to a restricted directory ("path traversal") |
| 68.5 | CWE-494 | Download of code without integrity check |
| 67.8 | CWE-863 | Incorrect authorization |
| 66.0 | CWE-829 | Inclusion of functionality from untrusted control sphere |
| 65.5 | CWE-732 | Incorrect permission assignment for critical resource |
| 64.6 | CWE-676 | Use of potentially dangerous function |
| 64.1 | CWE-327 | Use of a broken or risky cryptographic algorithm |
| 62.4 | CWE-131 | Incorrect calculation of buffer size |
| 61.5 | CWE-307 | Improper restriction of excessive authentication attempts |
| 61.1 | CWE-601 | URL redirection to untrusted site ("open redirect") |
| 61.0 | CWE-134 | Uncontrolled format string |
| 60.3 | CWE-190 | Integer overflow or wraparound |
| 59.9 | CWE-759 | Use of a one-way hash without a salt |

MITRE maintains the common weakness enumeration (CWE). For details of each software weakness, please visit cwe.mitre.org.

Lastly, software developers have many different methodologies and processes they prefer when they analyze, design, and implement their software. No matter which process they use, a few additional measures can be taken to help in the process of building secure software (Gregory 2010):

1. *Provide source code access control:* The only people with access to the source code should be authorized developers and even fewer people on the development team should be able to modify the source code.
2. *Provide protection of software development tools:* Reducing access and thus modification of the development tools and libraries will reduce the possibility of introducing vulnerabilities through tampering with the tools.

3. *Provide protection of the software development systems:* The servers used to house the source code repositories should be protected at the same level as the application servers. The hackers are looking for any weak link they can find.

## 3.9 Database Security

Databases are probably the most essential system a company owns. If a hacker is able to communicate with the company database, he now has access to business-critical data. The type of information that typical database systems house (customer, financial, and company details) can put the future of the business in question if that information gets into the wrong hands. Thus, engineers need to be aware of vulnerabilities and threats, attacks on databases, secure architectures, security models for the next generation of databases, security mechanisms in databases, security database design, and the attributes of database security. This is quite a challenge even for the most experienced, as we see in the news about stolen data from high-profile companies. In the previous section we showed the "Top 25 Most Dangerous Software Errors," where the SQL injection is number 1!

Database security is complex because it is not only about protecting against intentional theft or accidental exposure, but also about compromise of data by employee disgruntlement or ignorance. NIST (2011) suggests a data loss prevention (DLP) strategy that includes:

- Data inventory
- Data classification
- Data metric collection
- Policy development for data creation, use, storage, transmission, and disposal
- Tools to monitor data at rest, in use, and in transit

The preceding can be accomplished by using typical network and security tools such as network analysis software, application firewalls, and intrusion detection and prevention systems.

But how do we mitigate the number 1 problem of SQL injections where criminals are modifying database queries to steal, corrupt, and change private data?

The MITRE and SANS corporations suggest many specific prevention measures to mitigate SQL injection, including architecture and design decisions, implementation, and operation of the database in their CWE document cited in the previous section (http://cwe.mitre.org/top25/).

## 3.10 Business Continuity and Disaster Recovery

Business continuity and disaster recovery (BC/DR) planning includes both response and recovery plans as well as restoration activities if disaster occurs. Disasters can be anything from a virus to a hurricane or cyber attack. *Disaster recovery* includes a process that recovers critical information if a disaster happens to vital systems. *Business continuity* includes how the business will continue if the critical information is lost. An easy way to differentiate the two is that the BC is the process your company will follow in order to keep making money if disaster occurs. While the BC is in the works, the company can be performing DR, where the critical systems and information are recovered. Hence, one can appreciate why they both should be included in the same plan.

The essential pieces of the BC/DR plan will encompass how the immediate business needs can be met to resume operations. Generally, a plan would include the following (Dey 2011):

- Create a BC/DR team and define and assign roles to each team member.
- Conduct risk assessment to determine priorities and requirements.
- Create a plan including budget requirements.
- Create policies and procedures to be approved by management.
- Begin to implement the project (procure necessary resources).
- Arrange alternate network links and determine facility requirements (cold site, warm site, hot site). For example, the hot site would include the most resources (a fully configured computer facility).
- Achieve and maintain compliance, regulations, and best practices as they apply to your business.
- Link the BC/DR plan with the organization's change management process so that changes in the business process would be included in the BC/DR plan.
- Routinely test the plan.
- Review and iterate the BC/DR framework.

## 3.11 Physical Security

Securing the physical environment refers to addressing the security of the facility both internally and at the perimeter. This is defined as critical infrastructure protection—in other words, sections of the facility that provide protection and support of the critical information systems.

Following is a simplified view of the *priority 1* recommendations by NIST for the **physical and environment protection** baseline:

| | Impact Level | | |
|---|---|---|---|
| **Control Name** | **Low** | **Moderate** | **High** |
| Develop, distribute, and maintain physical and environmental protection policy and procedures | ✓ | ✓ | ✓ |
| Keep a current list of personnel authorized to access the facility | ✓ | ✓ | ✓ |
| Manage physical access control of the facility where information systems reside using devices and/or guards | ✓ | ✓ | ✓ |
| Access control for transmission medium within the facilities | | ✓ | ✓ |
| Access control for output devices (e.g., monitors, printers, audio devices) | | ✓ | ✓ |
| Monitor physical access | ✓ | ✓ | ✓ |
| Visitor control (authenticate individuals) | ✓ | ✓ | ✓ |
| Protect power equipment and cabling from damage | | ✓ | ✓ |
| Provide an emergency shutoff capability | | ✓ | ✓ |
| Provide short-term emergency power supply to shut down information systems properly in the event of primary power loss | | ✓ | ✓ |
| Provide emergency lighting in the event of a power outage | ✓ | ✓ | ✓ |
| Employ fire suppression and detection devices for information systems | ✓ | ✓ | ✓ |
| Implement temperature and humidity controls | ✓ | ✓ | ✓ |
| Provide water damage protection for information systems | ✓ | ✓ | ✓ |
| Monitor delivery area access | ✓ | ✓ | ✓ |
| Employ an alternate work site in the event of a security incident | | ✓ | ✓ |

## 3.12 Legal, Regulations, Compliance, and Investigations

In addition to technical experience, the cyber security professional needs to be familiar with the legal system and the many types of laws, regulations, and compliance as they pertain to information. This knowledge will help one to understand how to handle things like intellectual property and individual privacy, as well as how to conduct an investigation and handle evidence legally. These topics will be discussed in further detail in Chapter 6 but, for now, here are a few of the many laws and regulations with which a security professional should be acquainted:

- **Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act:** This act allows law enforcement to conduct electronic surveillance to investigate terrorists.

- **Privacy Act of 1974:** This act requires consent of a citizen for a person or agency to send information on that citizen.
- **Fourth Amendment:** This amendment to the Constitution states that the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996:** This act specifies safeguards (administrative, physical, and technical) to ensure the confidentiality, integrity, and availability of electronic health information.

## 3.13 Operations Security

Along with the other topics in this chapter, operations security also deals with a range of activities to minimize the risk of threats and vulnerabilities to the critical information of an organization. Operations security primarily entails identifying the information that needs protection and determining the most effective way to protect the information.

Understanding the key security operations concepts is a priority. An example is implementing access control mechanisms (discussed in Section 3.4) such as the concept of "need to know" where an individual only has access if the information is needed to perform his or her job. Another way to minimize risk is to implement "separation of duties," where no individual has control over an entire process, thus reducing the possibility of fraud. For example, changing a firewall rule should be performed by two people. The banking industry uses this concept in almost all of its processes; for example, no one person has the full combination to the bank vault. Thus, to open the vault you need two people, each knowing one-half of the combination. Other security operations concepts are rotating jobs (illegal activity would not likely be on the mind of a person being rotated out of a job) and monitoring special privileges to any type of system administrator (database, application, network), as he or she has the opportunity to corrupt data with privileged access.

Resource protection and incident response should also be considered as part of the operations security plan. The resources are physical entities such as hardware (e.g., equipment life cycle, cabling, and wireless networks) and software (e.g., licensing, access control, and source code protection). Incident response refers to a plan in place in the event that interruption of normal operations occurs. This plan would include how to detect and determine the type of incident, as well as a response, reporting, and recovery strategy. This will be covered in detail in an upcoming chapter.

Additional areas to consider are preventative measures against malicious attacks (e.g., DOS, theft, social engineering), patch and vulnerability management, configuration and change management (i.e., track all versions and changes to processes, hardware, software, etc.), and the fault tolerance of the components of any and all devices.

## 3.14 Information Security Governance and Risk Management

Information security governance is the organizational structure to implement a successful information security program. To apply security governance (e.g., processes, policies, roles, compliance, etc.), one must first understand the organization's goals, mission, and objectives. Once these are understood, one can identify the assets of the organization and implement an effective risk management plan using tools to assess and mitigate threats to and vulnerabilities of the asset.

Risk assessment can be accomplished either quantitatively, qualitatively, or both. A quantitative example is being able to put a dollar amount on a risk. For example, if 1,000 records of patient data were exposed and it costs $30 to contact a patient, change his or her account number, and print a new health card, then the loss with this risk is $30,000 (Sims 2012). A qualitative risk identifies characteristics about an asset or activity (Gregory 2010):

- **Vulnerabilities**: An unintended weakness in a product
- **Threats**: An activity that would exploit the vulnerability
- **Threat probability**: The probability that the threat will occur (low, medium, high, or a numeric scale)
- **Countermeasures**: Tools to reduce the risk associated with the threat or vulnerability

Other considerations include managing personnel security and developing security training and awareness. Secure hiring practices, such as performing reference checks, verifying education, and using employment agreements and policies between the employer and employee (e.g., nondisclosure) should be in place. In addition, once the person is hired, there should be security education, training, and awareness to mitigate risks. Training will be detailed in the "Preparing for an Incident" chapter.

In addition to software patches and fixes to protect against security vulnerabilities, sound judgment and caution are needed (Microsoft 2012). Here are the 10 immutable laws of security according to Microsoft:

> **Law #1:** *If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.*

**Law #2:** *If a bad guy can alter the operating system on your computer, it's not your computer anymore.*
**Law #3:** *If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.*
**Law #4:** *If you allow a bad guy to upload programs to your website, it's not your website anymore.*
**Law #5:** *Weak passwords trump strong security.*
**Law #6:** *A computer is only as secure as the administrator is trustworthy.*
**Law #7:** *Encrypted data are only as secure as the decryption key.*
**Law #8:** *An out-of-date virus scanner is only marginally better than no virus scanner at all.*
**Law #9:** *Absolute anonymity isn't practical, in real life or on the web.*
**Law #10:** *Technology is not a panacea.*

## References

Bowen, P., Hash, J., and Wilson, M. 2006. Information security handbook: A guide for managers. NIST special publication 800-100.

Conrad, E. 2011. *CISSP study guide.* Waltham, MA: Syngress.

Dey, M. 2011. Business continuity planning (BCP) methodology—Essential for every business. *IEEE GCC Conference and Exhibition*, February 19–22, pp. 229–232.

Evans, D., Bond, P., and Bement, A. 2004. Standards for security categorization of federal information and information systems. FIPS PUB 199, February 2004.

Felten, E. 2008. What's the cyber in cyber-security? Freedom to Tinker, July 24, 2008, https://freedom-to-tinker.com/blog/felten/whats-cyber-cyber-security/ (retrieved August 12, 2012).

Gregory, P. 2010. *CISSP guide to security essentials.* Boston: Course Technology, Cengage Learning.

Jaeger, T. 2008. *Operating systems security.* San Rafael, CA: Morgan & Claypool.

Khan, M., and Zulkernine, M. 2008. Quantifying security in secure software development phases. Annual IEEE International Computer Software Applications Conference.

King, R. 2009. Lessons from the Data Breach at Heartland. *Bloomberg Business Week,* July, 6, 2009, http://www.businessweek.com/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice (retrieved August 9, 2012).

Locke, G., and Gallagher, P. 2009. Recommended security controls for federal information systems and organizations. NIST special publication 800-53.

Martin, B., Brown, M., Paller. A., and Kirby, D. 2011. 2011 CWE/SANS top 25 most dangerous software errors. The MITRE Corporation.

Microsoft. 2012. 10 Immutable laws of security. http://technet.microsoft.com/library/cc722487.aspx (retrieved September 8, 2012).

Payne, J. 2010. Integrating application security into software development. *IT Professional* 12 (2): 6–9.

Sims, S. 2012. Qualitative vs. quantitative risk assessment. SANS Institute, http://www.sans.edu/research/leadership-laboratory/article/risk-assessment (retrieved December 27, 2012).

Swanson, M., and Guttman, B. 1996. Generally accepted principles and practices for securing information technology systems. NIST special publication 800-14.

Swanson, M., Hash, J., and Bowen, P. 2006. Guide for development of security plans for federal information systems. NIST special publication 800-18.

Talukder, A. K., Maurya, V. K., Santosh, B. J., Jangam, E., Muni, S. V., Jevitha, K. P., Saurabh, S., Pais, A. R. and Pais, A. 2009. Security-aware software development life cycle (SaSDLC)—Processes and tools. IFIP International Conference on Wireless and Optical Communications Networks. WOCN '09, pp. 1–5.

Theoharidou, M., and Gritzalis, D. 2007. Common body of knowledge for information security. *IEEE Security and Privacy* 5 (2): 64–67.

Title 44 United States Code Section 3542. US Government Printing Office. http://www.gpo.gov/fdsys/pkg/USCODE-2009-title44/pdf/USCODE-2009-title44-chap35-subchapIII-sec3542.pdf (retrieved August 15, 2012).

Tracy M., Jansen, W., Scarfone, K., and Butterfield, J. 2007. Guidelines on electronic mail security. NIST special publication 800-45.

Vijayan, J. 2010. Update: Heartland breach shows why compliance is not enough. Computerworld, http://www.computerworld.com/s/article/9143158/Update_Heartland_breach_shows_why_compliance_is_not_enough (retrieved August 9, 2012).

Whitman, M., and Mattord, H. 2012. *Principles of information security.* Stamford, CT: Cengage Learning, Course Technology.

# 4

# *Preparing for an Incident*[*]

> Before anything else, preparation is the key to success.
>
> **—Alexander Graham Bell**

## 4.1 Introduction

As my father-in-law has said, "If you don't prepare the garden in the spring it won't be ready to harvest in July." Preparing does not just include turning the ground over and planting the seeds; it also includes putting up a fence and using deterrents for those pesky deer and rabbits trying to eat everything. If we apply that sentiment to security incidents, the information security professional obviously needs much more than a firewall to deter those pesky hackers from our critical data and systems as was outlined in the previous chapter. In addition, the digital forensics professional also needs the security deterrents set up in such a way that they will have the appropriate means to help catch and convict the intruder if he or she does get unauthorized access. The digital forensic process also needs to be able to gather information to determine and secure the vulnerability that was exploited. Thus, in this chapter, the topics and safeguards that needed to be implemented preincident to facilitate securing the assets as well as provide data for an effective investigation postincident will be discussed.

It can be an overwhelming task for any business—well aware of the exponentially growing cyber threats to its critical assets—to maintain a comprehensive security posture. A comprehensive security posture will include features that will not only mitigate incidents but will also make both incident response (IR) and the digital forensic investigation much more effective because all bets are that the incident will occur eventually and will need to be investigated. In other words, just as in firing a weapon, "aim, fire" is not enough, the weapon should be "ready" too. In an organization in which resources are tight, preincident preparation and the development of the IR process may take a back seat to responsibility of securing the system. The point is that a successful preincident preparation process should have its own focus by *both* the information security *and* digital forensics professionals to

[*] Excerpts in this chapter are from DeFranco and Laplante (2011).

reduce the cost and increase the success of an investigation. In particular, this focus will help ensure that policies are followed and that data collected can be used as evidence in a court of law if necessary.

I chose to present this topic using a framework that can help communicate how a company can prepare to protect its infrastructure and critical data from cyber threats as well as be in a position to perform an effective digital forensic investigation if and when an incident occurs. The proposed framework is notably derived from the Zachman enterprise architecture (Zachman 1987).

### 4.1.1 The Zachman Framework

The widely used Zachman framework (Figure 4.1), developed by John Zachman in 1987, provides a way to rationalize architectural concepts and facilitate communication among the designers of complex information systems. The Zachman framework can be adapted to model a variety of complex systems.

In the figure, the six dimensions shown as the rows in the framework represent different stakeholder perspectives of a complex system. Essentially, the framework lays out the architectural model including each stakeholder in a system, thus creating a complete view of that system. Zachman's main goal was to emphasize the fact that systems design is not just about the system itself; instead, it is an enterprise issue.

The columns in the framework are a metamodel that answers the questions, what, how, when, who, where, and why to describe the enterprise.

### 4.1.2 Adaptation of the Zachman Framework to Incident Response Preparation

The only reported application of the Zachman framework to digital forensics is Leong's (2006) FORZA model. In this case, Leong used Zachman to define eight different roles and responsibilities in a digital forensic investigation via a set of interrogative questions that can be utilized during an investigation. While Leong's model provides a rigorous way to approach postincident data collection, the FORZA model does not address the issue of preparation, which will have an effect on the success of the investigation. Mandia, Prosise, and Pepe (2003), a highly cited resource in incident response, recommended six areas to be addressed in preincident preparation: identifying risk, preparing hosts, preparing networks, establishing policy/procedure, creating a response toolkit, and creating a team to handle incidents. With the addition of a new dimension, *training,* coupled with several special publications of the NIST (National Institute of Standards and Technology) and a few other resources, the Zachmam framework is modeled for the digital forensics preparation process (DeFranco and Laplante 2011). This new framework provides a model to analyze the vulnerabilities critically, gives suggestions for security and education, and presents a plan for the overall protection of an enterprise's resources, data, and information.

| | DATA *What* | FUNCTION *How* | NETWORK *Where* | PEOPLE *Who* | TIME *When* | MOTIVATION *Why* | |
|---|---|---|---|---|---|---|---|
| SCOPE (CONTEXTUAL)<br>*Planner* | List of Things Important to the Business<br>ENTITY = Class of Business Thing | List of Processes the Business Performs<br>Function = Class of Business Process | List of Locations in which the Business Operates<br>Node = Major Business Location | List of Organizations Important to the Business<br>People = Major Organizations | List of Events Significant to the Business<br>Time = Major Business Event | List of Business Goals, Strat<br>Ends/Means = Major Bus. Goal/ Critical Success Factor | SCOPE (CONTEXTUAL)<br>*Planner* |
| ENTERPRISE MODEL (CONCEPTUAL)<br>*Owner* | e.g. Semantic Model<br>Ent = Business Entity<br>Reln = Business Relationship | e.g. Business Process Model<br>Proc. = Business Process<br>I/O = Business Resources | e.g. Logistics Network<br>Node = Business Location<br>Link = Business Linkage | e.g. Work Flow Model<br>People = Organization Unit<br>Work = Work Product | e.g. Master Schedule<br>Time = Business Event<br>Cycle = Business Cycle | e.g. Business Plan<br>End = Business Objective<br>Means = Business Strategy | ENTERPRISE MODEL (CONCEPTUAL)<br>*Owner* |
| SYSTEM MODEL (LOGICAL)<br>*Designer* | e.g. Logical Data Model<br>Ent = Data Entity<br>Reln = Data Relationship | e.g. "Application Architecture"<br>Proc. = Application Function<br>I/O = User Views | e.g. "Distributed System Architecture"<br>Node = I/S Function (Processor Storage, etc.)<br>Link = Line Characteristics | e.g. Human Interface Architecture<br>People = Role<br>Work = Deliverable | e.g. Processing Structure<br>Time = System Event<br>Cycle = Processing Cycle | e.g., Business Rule Model<br>End = Structural Assertion<br>Means = Action Assertion | SYSTEM MODEL (LOGICAL)<br>*Designer* |
| TECHNOLOGY MODEL (PHYSICAL)<br>*Builder* | e.g. Physical Data Model<br>Ent = Segment/Table/etc.<br>Reln = Pointer/Key/etc. | e.g. "System Design"<br>Proc. = Computer Function<br>I/O = Screen/Device Formats | e.g. "System Architecture"<br>Node = Hardware/System Software<br>Link = Line Specifications | e.g. Presentation Architecture<br>People = User<br>Work = Screen Format | e.g. Control Structure<br>Time = Execute<br>Cycle = Component Cycle | e.g. Rule Design<br>End = Condition<br>Means = Action | TECHNOLOGY CONSTRAINED MODEL (PHYSICAL)<br>*Builder* |
| DETAILED REPRESEN-TATIONS (OUT-OF-CONTEXT)<br>*Sub-Contractor* | e.g. Data Definition<br>Ent = Field<br>Reln = Address | e.g. "Program"<br>Proc. = Language Stmt<br>I/O = Control Block | e.g. "Network Architecture"<br>Node = Addresses<br>Link = Protocols | e.g. Security Architecture<br>People = Identity<br>Work = Job | e.g. Timing Definition<br>Time = Interrupt<br>Cycle = ??? Cycle | e.g. Rule Specification<br>End = Sub-condition<br>Means = Step | DETAILED REPRESEN-TATIONS (OUT-OF-CONTEXT)<br>*Sub-Contractor* |
| FUNCTIONING ENTERPRISE | e.g. DATA | e.g. FUNCTION | e.g. NETWORK | e.g. ORGANIZATION | e.g. SCHEDULE | e.g. STRATEGY | FUNCTIONING ENTERPRISE |

**FIGURE 4.1**
The Zachman framework.

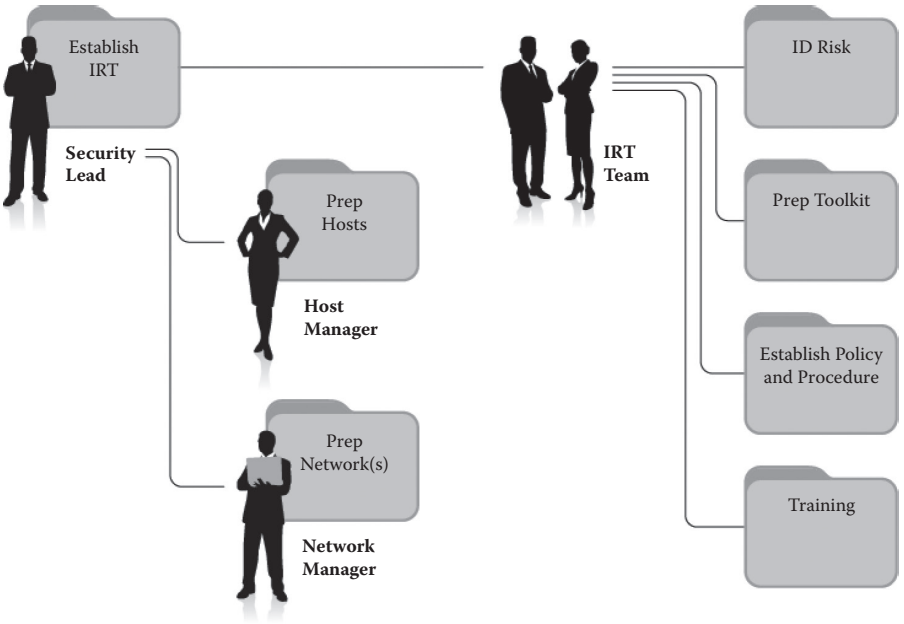



**FIGURE 4.2**
Package diagram of the preincident prep framework.

In the case of preincident preparation, these seven abstraction layers can be derived by analyzing the package diagram shown in Figure 4.2.

Table 4.1 illustrates the areas that were adapted by applying the Zachman framework as well as the factors that are of interest to prepare effectively for an incident.

The following sections will highlight the activities described in Table 4.1 in further detail. Section headings correspond to row headings in the table, and the italicized questions are fully realized versions of the factor list in the second column of the table.

## 4.2 Risk Identification

***Why** do we need to evaluate security threats continuously?*

The enterprise must contend with malware, vulnerabilities in their applications, user mobility, spam, even its employees—the list could go on and on. Due to the ever-changing nature of the threat space, it is impossible to determine every vulnerability in

**TABLE 4.1**

Preincident Prep Model

| Layers | Factors |
|---|---|
| • Identifying risk | • **Why** do we need to evaluate security threats continuously?<br>• **Wha**t is a risk?<br>• **What** are the critical assets? Which parts of the system need to be secured?<br>• **Where** are the critical assets?<br>• **Who** has access to mission-critical data?<br>• **When**/how often should risks be evaluated?<br>• **How** is risk assessment performed? |
| • Preparing individual hosts (a computer connected to the network) | • **Why** do the host computers need continuous monitoring?<br>• **What** activities can protect the host?<br>• **What** application software needs to be patched?<br>• **What** data are critical and should be backed up and secured?<br>• **When** should backups be scheduled?<br>• **Who** will lead the host-based security effort?<br>• **Where** are the host computers are located?<br>• **Who** needs to be educated on host-based security?<br>• **Who** has access to the hosts?<br>• **How** can data be protected while using cloud services? |
| • Preparing the network | • **Why** does the network need continuous monitoring?<br>• **Who** will manage this effort?<br>• **What** activities can protect the network?<br>• **When** did the events occur? Network synchronization.<br>• **Where** did the incident occur?<br>• **How** to prepare for an advanced persistent threat (APT) |
| • Establishing appropriate policies and procedures | • **What** is an acceptable use policy (AUP)?<br>• **Why** do we need an AUP?<br>• **Who** is affected by the AUP?<br>• **How** do we determine what the AUP should address?<br>• **When** and how often should the AUP be updated?<br>• **Where** should the AUP document be kept? |

(*Continued*)

**TABLE 4.1 (*Continued*)**

Preincident Prep Model

| Layers | Factors |
|---|---|
| • Creating/preparing response tools kit | • **Why** is a response toolkit necessary?<br>• **When** is the response toolkit used?<br>• **Where** is the toolkit used?<br>• **How** is the toolkit assembled?<br>• **What** is the necessary hardware, software, and documentation needed to respond to incidents? |
| • Establishing an incident response team | • **Why** do we need to establish a response team?<br>• **Who** should be on the computer incident response team (CIRT)?<br>• **How** to establish a CIRT?<br>• **When** should stakeholders be contacted?<br>• **What** factors need to be considered in creating a CIRT?<br>• **Where** is the incident evidence stored? |
| • Training | • **Why** is it important to educate the users?<br>• **Who** will do the training?<br>• **Where** should the training occur?<br>• **When** should the training occur?<br>• **How** should the users be trained?<br>• **What** should the users be trained on? |

a network; however, by determining and addressing the known vulnerabilities, the enterprise can be prepared both offensively and defensively.

An effective approach to improving an organization's security posture and preventing incidents is to conduct periodic risk assessments of systems and applications (Grance, Kent, and Kim 2004). Assessing risk is clearly the first step in improving a company's security posture.

***What** is a risk?*

A risk is the probability that a threat will take advantage of a system's vulnerability.

***What** are the critical assets (i.e., which parts of the system need to be secured)? Where are the critical assets located? **Who** has access to mission-critical information/data?*

Critical assets pertain to confidential customer or company data, critical plans, private individual data, or even the corporate reputation. Anything that, if stolen or compromised, would be harmful to the company's future is considered a risk. Although

large networks can be vulnerable to hackers, defenders also need to worry about the malware located everywhere on the Internet that their users are perusing as well as external threats getting to the critical assets. Thus, the threats faced by most organizations now have an additional focus on internal users. Those users are a big risk due to their privileged access to confidential information as well as their access to critical applications.

Creating and documenting the a network topology can also assist in the risk assessment effort. The topology will show where the critical assets are located and how they are connected. This view can highlight vulnerabilities that need to be addressed.

***When****/how often should risks be evaluated?*

Risks evolve, networks change, and people leave—all reasons why the risks need to be evaluated as often as possible. Vulnerability risk evaluation should be run weekly for optimum security and monthly—at least—for best practice (NTT 2009).

***How*** *is a risk assessment performed?*

NIST suggests the following risk assessment methodology (Stoneburner, Goguen, and Feringa 2002):

1. *System characterization:* Understand the system topology and gather information to determine the system's environment and boundary.
2. *Threat identification:* Determine a list of threat sources that may exploit any of the system vulnerabilities or an action that may unintentionally initiate exploitation of a vulnerability. A threat-source can be a hacker, a criminal, or even a poorly trained or unhappy employee.
3. *Vulnerability identification:* Determine the weaknesses that could be exploited. There are many known vulnerabilities that can be found through vulnerability databases,* vendors, vulnerability-scanning tools, and penetration testing. Other vulnerabilities can be found by assessing the security requirements of the system itself.
4. *Control analysis:* Determine controls to minimize the probability of a security incident. Many of the access control techniques, such as authentication and encryption discussed in Chapter 3, are controls that may be utilized to minimize incidents.
5. *Likelihood determination:* To determine the likelihood of a threat source exercising the vulnerability, consider the motivation and capability of the threat source, the nature of the vulnerability,

* National Vulnerability Database: http://web.nvd.nist.gov/view/ncp/repository.

and the access controls in place. The likelihood can be rated as *high, medium,* or *low.*

6. *Impact analysis:* Determine the magnitude of the impact. An impact analysis as was described in Chapter 3 can be implemented to determine the effect of the incident on the integrity, availability, and confidentiality of the system and data. The impact can be rated as *high, medium,* or *low.*
7. *Risk determinations:* Determine the level of risk that the threat source will take advantage of the vulnerability by evaluating the likelihood of an attempt, the magnitude of the impact, and the effectiveness of the security controls.
8. *Control recommendations:* Determine effective controls and alternate solutions to reduce risk probability. These determinations should consider the effectiveness of the options, legislation/regulation, organization policy, operational impact, safety, and reliability.
9. *Results documentation:* Assemble an official report describing the analysis.

The Ponemon Institute surveyed fifty six US organizations where the results showed that the cost of cyber crime averaged $8.9 million. This is a 6 percent increase over the 2011 study. Those companies experienced an average of 1.8 successful attacks per week—a 42 percent increase from 2011. The most common attacks are denial of service (DOS), malicious insiders (permanent and temporary employees, contractors, and business partners), and web-based attacks. Figure 4.3 depicts the comparison of the US cyber crime cost average against those of four other countries.

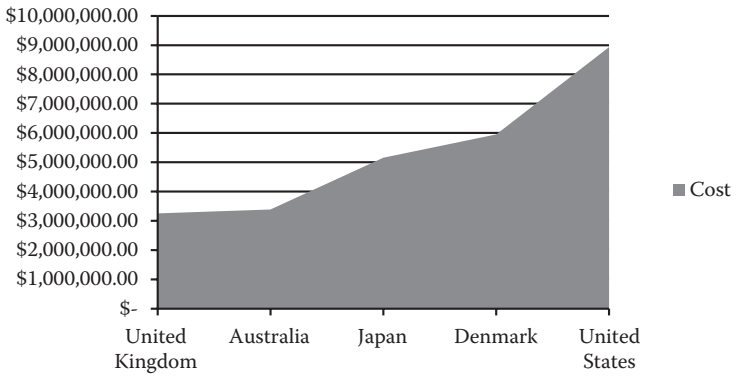



**FIGURE 4.3**
Cybercrime cost comparison of five countries. (Adapted from Ponemon Institute, 2012, http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf).

## 4.3 Host Preparation

***Why** do the host computers need continuous monitoring?*

With the growth of mobile computing, there are many devices connected to the network. Devices that are connected to corporate networks now have access to sensitive data. In addition, they all connect to the Internet, cloud services, and social networking sites that are all significant contributors to security incidents.

***What** activities can protect the host?*

NIST recommends several important practices for securing a host, such as limiting user privileges, evaluating default settings and passwords, displaying warning banners for unauthorized use, and enabling logging (useful for incident investigations) of significant security-related events (Grance et al. 2004).

Believe it or not, user password choice continues to be a problem. For example, Yahoo Voices, an open- publishing platform, had 453,491 plaintext passwords and e-mail addresses stolen (Brading 2012). The hacking was due to a structured query language (SQL) injection. What was discovered is a good reminder of why passwords need to be evaluated. These stolen passwords were FAR from secure; for example, 1,373 people used "password" as their password and 1,666 used "123456" (Cluley 2012). This is a shocking reality; therefore, users need to be forced, via password management software, to use strong passwords. In addition, passwords should never be stored in plaintext. They should be salted (add a random string of characters prior to hashing), hashed, encrypted, and protected in a password database (Brading 2012). If password management software is not available to force users to create strong passwords, there are some simple password creation tips that may be effective to share with the users, such as using eight characters or more, not using personal information, using a mix of numbers and upper- and lowercase letters, and to avoid dictionary words or those words spelled backward. In addition, encourage users to vary passwords across accounts.

*Another host protection activity is simply updating application software with any and all updates.*

Many cyber attacks are directed at heavily used applications such as word processors or reader applications. The patch alerts targeted toward users are often ignored. Simply installing security patches can avoid some of the malicious code that, when installed on a host machine, can spread spam, steal data, or take control of the host. NIST (2004) suggests that organizations should implement

a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches. In addition, a good practice is archiving known vulnerabilities, patches, or resolutions of past problems (Brownlee and Guttman 1998).

***What*** *data are critical and thus should be backed up and secured? Which files are critical and therefore need a cryptographic check sum recorded? When should backups and check sum updates be scheduled?*

A cryptographic checksum is a hash value produced by running an algorithm on a particular file. Essentially, all of the bits of data in a particular document or file are added up and a number or "hash value" is created. This hash value can then be compared to the hash value generated from the same file on another person's computer or at a previous time on the same computer. Preparation should include determining which files are critical and thus need some form of authentication signature, such as a checksum. These values need to be backed up and secured along with the files. If updates to these critical files occur, a new checksum needs to be produced.

***Who*** *will lead the host-based security effort?* ***Where*** *are the host computers located?* ***Who*** *needs to be educated about host-based security?* ***Who*** *has access to the hosts?*

Whoever is leading the host-based security effort also needs to determine and document where the host computers are located (discussed in risk section) as well as who has access to the host computers. The host-based security lead should also facilitate an education program for host-based security.

***How*** *can data be protected while using cloud services?*

Cloud services can be a risk. Sophos (2013) suggests the following steps to protect data on the cloud:

1. Apply URL filtering as part of the web-based policy. This will prevent use of public cloud storage websites as well as other sites deemed prohibited.
2. Control access to particular applications.
3. Files should be automatically encrypted prior to uploading to any cloud storage service. This encryption will be instrumental to the safety of your files if the cloud provider has a security breech.

Not all threats come from the outside and certainly not all of the system vulnerabilities are from your network. If a company has a trade secret such as a process, formula, or a software application that needs to be protected, that company needs to consider how to protect that asset from employee theft. A 2012 survey from Cyber-Ark Software interviewed 820 IT professionals in an attempt to identify security trends. The survey revealed

that 55 percent of the respondents feel their intellectual property has been obtained by their competitors. In addition, nearly half of the respondents indicated that they would take something with them if they knew they were going to be fired tomorrow, such as an e-mail server admin account, financial reports, customer database, privileged password list, etc. What if the person knew he or she was quitting? Should the person stop attending strategic meetings? Not open sensitive files? YES—especially if he or she is one of seven people in the world who know a trade secret such as a recipe to an extremely popular baked product. This happened to Bimbo Bakeries, the maker of Thomas's English muffins. A top executive took a job offer from a competitor; however, prior to his exit, he accessed sensitive files such as cost-cutting strategies and labor contracts—information that could be damaging to Bimbo in the hands of a competitor (Dale 2010). Thus, this situation ended up in a trade secret fight. The executive was ordered not to work for the competitor, prohibited from divulging Bimbo's trade secrets, ordered to return confidential information, and ordered to notify Bimbo if he accepted employment in the baking industry (Lewis and Roca, LLP 2011).

## 4.4 Network Preparation

***Why** does the network need continuous monitoring? **Who** will manage this effort?*

It is obvious why we need to monitor our networks continuously, but it is absolutely worth repeating. Refer back to Figure 1.1, which shows the increase of attack sophistication and the decrease of attacker knowledge needed to be destructive. The FBI reports that early in 2012 hackers embedded malicious software in *two* million computers. Accordingly, our networks need to be prepared to protect our data privacy, integrity, and availability. This section will cover some of the tasks a security professional can perform in order to improve the security profile of a network.

***What** activities can protect the network?*

*Encrypt network traffic.* All data traveling across a network should be encrypted. For example, e-mail should have the content encrypted as well as all attachments to ensure their integrity. These e-mails are stored on multiple servers, included on backups, and inspected by firewalls. Traffic sniffers should also monitor where these e-mails might be stored or travel.

*Vulnerability management.* There are many aspects to analyzing the vulnerabilities of the network. Nearly all incidents involving vulnerability exploits could have been avoided (NTT 2009). Generally, vulnerability scans are performed on the system to determine where it is weak. Also, companies need to be aware that any open ports on the firewall are exposing the system to the outside world. Mobile devices such as USB drives and phones

are also a risk. Applications need to be tested since hackers are now exploiting those as well as the operating system in which they are running.

*Internal risks.* In addition to external risks outside the firewall such as malware and hackers, companies also need to be concerned with internal breaches to their network. There are applications to monitor sensitive data as well as a specific user status. It is also important to identify which groups of users on the network have access to which types of information (National Security Agency 2009).

*Network synchronization—an accurate determination of **when** events occur.* With respect to forensic investigations, timing is very important. In a digital investigation, having the networks in sync will ease the investigators in determining when everything happened. Many organizations use a publically available time server or install a time server behind the firewall. A downside of a public time server is that it leaves a hole in the firewall. A private time server is expensive. When using a cloud configuration, synchronized time becomes even more imperative. The forensics performed on a cloud configuration will be easier to defend if the time stamps from the client-side log files match the time stamps on the provider-side log files (Zimmerman and Glavach 2011).

*Install intrusion detection and prevention systems (IDS/IPS), firewalls, and require authentication.* The network perimeter needs to be configured so that it denies activities not expressly permitted, such as any violation of the company's security policies. To secure the network perimeter, firewalls, IDS, and/or IPSs are typically employed. Depending on the settings, a firewall can block or allow traffic coming from an Internet or network. The drawbacks of a firewall are that the firewall cannot prevent attacks from the intranet, the firewall policy is not dynamic in that it cannot change depending on the attack, and the firewall rules are too simplistic to prevent a virus (Zhang, Li, and Zheng 2004). Thus, in addition to a firewall, an effective network security plan may use an IDS/IPS solution. An IDS monitors the network by looking for any signs of a possible incident. However, the alert will sound after the problem has passed through. An IPS can do the work of an IDS but it can also attempt to stop an incident by preventing access to the network. The NIST "Guide to Intrusion Detection and Prevention Systems" (SP800-94) contains extensive information on IDS/IPS technologies as well as implementation recommendations. Essentially, requiring authentication and installing firewalls and intrusion protection systems should

secure network connection points to the organization. The goal is to prevent intrusions, viruses, and zero-day attacks (brand new vulnerabilities that no one knew about) based on rules and packet inspection.

***Where** did the incident occur?*

As mentioned in the past two sections, knowledge of the network topology will assist in determining the location of the affected systems and servers when an incident occurs. An effective way to document the network topology is by using a blog or bulletin board to notify administrators of changes as well as a wiki to document the network topology (National Security Agency 2009). In this case, however, it is important that the actual network map is in a secure location. Some other information resources that should be included are commonly used ports, operating system documentation, baselines of network and application activity, and hashes of critical files (Grance et al. 2004).

***How** to prepare for an advanced persistent threat (APT):*

The way to be prepared for an APT is first to know how to diagnose an APT. An APT is an attack where hackers infiltrate the corporate network and steal sensitive data over a long period of time. These types of hackers are in it for more than the quick buck they could make through identity theft attacks. They are there to steal big secrets, which may take a considerable amount of time. Roger Grimes, a security advisor at InfoWorld, describes an APT as attackers who "exploit dozens to hundreds of computers, logon accounts, and e-mail users, searching for new data and ideas over an extended period of months and years." Traditional methods of attack are often mistaken for APTs. The five signs that you've been hit with an APT are (1) an increase in elevated logons at night (hackers may live in another time zone), (2) widespread backdoor Trojans (a malicious application), (3) unexpected information flows (which can be from one inside computer to another), (4) unexpected data bundles (all stolen data are bundled prior to moving them to the hacker's desired location), and (5) hacking tools that were left behind (such as tools to steal hash numbers) (Grimes 2010).

The next step is to use a defense model that takes into consideration the process the APT attackers use. A team at Lockheed Martin created a model to deal with APT threats. They describe the stages (Figure 4.4) of the attack as a "kill chain." The idea is to use an approach to "stalk the kill chain" by watching the network and being able to identify the kill chain events (Cox 2012). In other words, watch the network as a whole instead of looking at events in isolation.

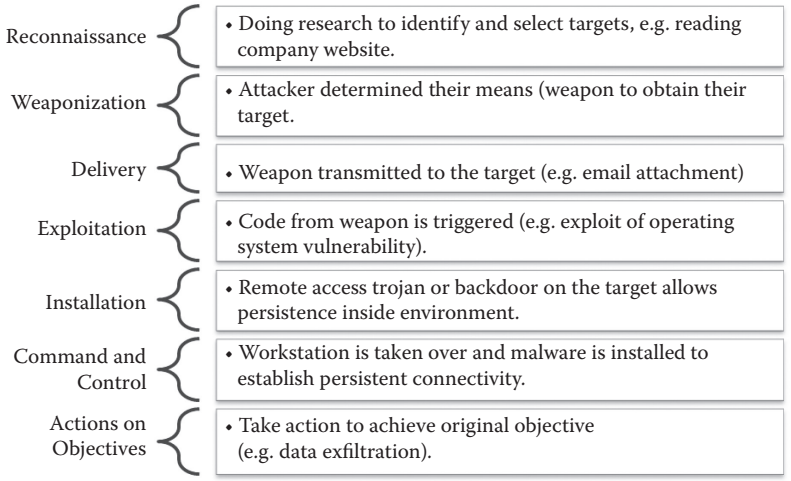



**FIGURE 4.4**
Kill chain stages.

## 4.5 Establishing Appropriate Policies and Procedures

*Develop and update an acceptable use policy (AUP).*

***What** is an AUP? **Why** do we need it? **Who** is affected by the AUP? **How** do we determine what the AUP should address? **When** and how often should it be updated? **Where** should the AUP document be kept?*

An AUP is a document containing an extensive set of rules that restrict how the network and resources may be used. A company can reduce the risk of litigation by publishing and maintaining corporate policies that outline the acceptable use of company resources. An AUP should also outline the policy to prevent malware (e.g., scanning media from the outside, scanning e-mail file attachments, forbidding sending or receiving .exe files, restricting the use of unnecessary software that is often used to transfer malware, restricting removable media, etc.) (Mell, Kent, and Nusbaum 2005). The AUP can also help to protect trade secrets. For example, confidential information e-mailed outside the organization may be prohibited. To monitor such events, the security team implements the necessary hardware and software. In addition, the "rule" (transmission of confidential information outside the company is prohibited) is written into the company AUP. If an employee attempts to e-mail a confidential document outside the company, an alarm is triggered and the security team investigates.

**An Example**

An employee needs to distribute a confidential presentation file to several of the company sites. The presentation was created on a PC. The employee is aware that a few of the people viewing the presentation will be using a Mac and is concerned that the presentation file may not function properly in a Mac OS. To save herself the hassle of hunting down a Mac user at work, she innocently e-mails the file to her personal e-mail address to test the presentation on her personal Mac computer. The e-mail was sent, the firewall was tripped, and within minutes she gets the following email:

---

**From: Mail Delivery Subsystem <MAILER-DAEMON@<companyname>.com**

**Date: Friday, Mar 1, 2013 5:06 PM**

**Subject: Returned mail: see transcript for details**

Dear Sender:

We have blocked your request to send this e-mail outside the company's firewall.

Please be aware that transmitting this type of content outside the company without prior express authorization may be a violation of company policy.

Do not attempt to retransmit this information in any other form. Sending <company name> confidential information outside the company may violate our policy and may subject you to discipline, up to and including termination of employment.

If you think you have received this message in error, please forward the content of your original message, including who you are sending it to, along with a brief explanation of why your message needs to be sent outside the company to emailprt@<companyname.com>. Your request will be reviewed in a timely manner.

Please contact us with any questions

Regards,

<Company Name> Information Protection Services

---

Figure 4.5 shows an excerpt of an example AUP provided by Sophos, an IT security and data protection provider.

Once the AUP is created and available (usually on the company intranet), it needs to be updated and enforced. The company should require that the AUP be read by all new hires and require a signature prior to using any computer resources at the company. It may also be effective to have the AUP reread annually, as it should be updated and reflect the current trends in technology.

For example, many companies needed to address the bring-your-own-device (BYOD) trend in their AUPs. Just as in anything, there are pros and cons with BYOD. If not addressed properly, it can be an issue for both the employee and the employer. Here are the pros and cons of BYOD (Bradley 2011):

*Pros:* The users are incurring the cost of the device and the associated expenses (e.g., voice and data). The satisfaction of the users will also increase because they are choosing the brand and model of

***Example Policy***

**1. Introduction**

This acceptable use policy (AUP) for IT Systems is designed to protect <Company X>, our employees, customers, and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g., computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at <Company X> is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts his or her role, he or she should speak to his or her manager or IT security officer.

**2. Definitions**

"Users" are everyone who has access to any of <Company X>'s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers, and business partners.

"Systems" means all IT equipment that connects to the corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically stored data, portable data storage devices, third-party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

**3. Scope**

This is a universal policy that applies to all users and all systems. For some users and/or some systems, a more specific policy exists. In such cases, the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of <Company X>'s systems and does not cover use of our products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws). In such cases, the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases, local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at <Company X> who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

**4. Use of IT Systems**

All data stored on <Company X>'s systems is the property of <Company X>. Users should be aware that the company cannot guarantee the confidentiality of information stored on any <Company X> system except where required to do so by local laws.

<Company X>'s systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users' own or their colleagues' productivity, nor should it result in any direct costs being borne by <Company X> other than for trivial amounts (e.g., an occasional short telephone call).

**FIGURE 4.5**
Sophos example IT AUP (http://www.sophos.com).

<Company X> trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain, they should consult their manager.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent—or risk preventing—legitimate access by all properly authorized parties.

<Company X> can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the e-mail and data files of any user, and examination of the access history of any users.

<Company X> reserves the right to audit networks and systems regularly to ensure compliance with this policy.

**5. Data Security**

If data on <Company X>'s systems is classified as confidential, this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgment when deciding which information is confidential.

Users must not send, upload, remove on portable media, or otherwise transfer to a non-<Company X> system any information that is designated as confidential, or that they should reasonably regard as being confidential to <Company X>, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with <Company X>'s safe password policy.

Users who are supplied with computer equipment by <Company X> are responsible for the safety and care of that equipment and the security of software and data stored on it and on other <Company X> systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets, and smartphones, is especially vulnerable, special care should be exercised with these devices: Sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after, at most, 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must, at all times, guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into <Company X>'s systems by whatever means and must report any actual or suspected malware infection immediately.

**FIGURE 4.5 (*Continued*)**

**6. Unacceptable Use**

All employees should use their own judgment regarding what is unacceptable use of <Company X>'s systems. The activities below are provided as examples of unacceptable use; however, the list is not exhaustive. Should an employee need to contravene these guidelines in order to perform his or her role, the employee should consult with and obtain approval from his or her manager before proceeding:

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of <Company X>. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities only for personal benefit that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- All activities that are inappropriate for <Company X> to be associated with and/or are detrimental to the company's reputation. These include pornography, gambling, inciting hate, bullying, and harassment.
- Circumventing the IT security systems and protocols that <Company X> has put in place.

**7. Enforcement**

<Company X> will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Use of any <Company X>'s resources for any illegal activity will usually be ground for summary dismissal, and <Company X> will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

**FIGURE 4.5 (*Continued*)**

the device they are bringing to work. They are also updating their devices to the latest and greatest technology much sooner than the organization would.

*Cons:* The company is losing control over the hardware and how the devices are utilized. The AUP and compliance mandates are more difficult to enforce since the device is not company owned. There is also the issue of when the employee separates from the company: The company wants its data back! This will get very tricky if there is a lawsuit involved; the employee may think that his or her phone does not need to be examined, but that is probably not the case. This risk needs to be explained to employees participating in a BYOD program.

Mobile phones are the most popular device to bring. Most mobile devices, especially user-owned mobile devices, can be untrustworthy and do not have many of the trust features that are built into hosts and laptops (Souppaya and Scarfone 2012). NIST (2012) suggests running the

organization's software in a secure state (in isolation from the rest of the device's applications and data) on the mobile phone or utilizing integrity scanning applications for that specific device. Important factors when developing a mobile device security policy include: sensitivity of the work, level of confidence in security policy compliance, cost, work location, technical limitations (if the device needs to be able to run a particular application), and compliance with mandates and other policies (Souppaya and Scarfone 2012).

Other things to consider when writing a BYOD policy (Hassell 2012) include:

1. **Specify what devices are permitted** and supported by the organization.
2. **Establish a stringent security policy for all devices,** such as a complex password attached to the device.
3. **Define a clear service policy for devices under BYOD criteria,** such as support for applications, broken devices, initial connections, etc.
4. **Make it clear who owns which applications and data** because if the device becomes lost or stolen, the company may wipe the device for security reasons—thus, personal data will be gone. Possibly provide information to the employee regarding backing up his or her own content.
5. **Decide which applications will be allowed or banned.** More than a few mobile device applications have vulnerabilities.
6. **Integrate your BYOD plan with your AUP.** Address social networking, viewing objectionable websites, and how its use will be monitored while a device is connected to the corporate network.
7. **Set up an employee exit strategy** to address how access tokens, e-mail access, data, and proprietary applications and information will be removed.

## 4.6 Establishing an Incident Response Team

***Why** do we need to establish a response team?*

There is no question that computer incidents are on the rise and that organizations need all the help they can get to be prepared. The computer incident response team (CIRT) is the much needed point of contact when an incident occurs. The CIRT can help determine the incident's impact on the organization as

well as perform tasks that can mitigate the damage and get the organization up and running again. They can also help with risk assessment, offer lessons learned, and help with training.

***Who** should be on the CIRT?*

Depending on the needs of the organization, the team can consist of employees, be fully outsourced, or be a combination of the two. This choice will depend on the organization's resources and needs.

NIST has written a "Computer Security Incident Handling Guide" (Cichonski et al. 2012) that addresses the CIRT. It contains CIRT recommendations that address ***what*** factors need to be considered, ***how*** to establish the team, ***when*** to contact stakeholders, etc.:

- Establish a formal incident response capability to be prepared when there is a breach.
- **Create an incident response policy** to define "incidents," roles, and responsibilities, etc.
- **Develop an incident response plan based on the incident response policy.** Also, establish metrics to assess the program and how training should occur.
- **Develop incident response procedures** that detail the step-by-step process of responding to an incident.
- **Establish policies and procedures regarding incident-related information sharing** such as media, law enforcement, etc. The team needs to consult with the organization's legal department, public affairs, and management to determine the policy and procedure.
- **Provide pertinent information on incidents to the appropriate organization,** such as the US-CERT for federal civilian agencies and/or ISAC organizations who use data to report threats and incidents.
- **Consider the relevant factors when selecting an incident response team model** to construct the most effective team structure (e.g., to outsource or not) for the organization.
- **Select people with appropriate skills for the incident response team.** In addition to technical skills, being able to effectively communicate should be a requirement.
- Identify other groups within the organization that may need to participate in incident handling, such as management, legal, facilities, etc.
- **Determine which services the team should offer** in addition to incident response, such as monitoring intrusion detection sensors, disseminating information regarding security threats, and educating users on the security policies.

In addition to the preceding, are a few other elements to consider when building an effective CIRT team:

*Train the response team **(what).***

Given the technology growth rate, the CIRT team will probably need additional training. A properly trained team is as important as having a secure network, as it will increase the chances of data validity upon collection. In general, the response team is responsible for facilitating technical assistance (analyzing compromised systems), eradication (elimination of the cause and effect of incidents), and recovery (restoring systems and services) (Brownlee and Guttman 1998). Outside training involving certifications (as discussed in Chapter 2) is an option to educate the team effectively on procedure, process, and documentation. A major part of this training should be learning how to ensure the integrity of the evidence. This will be discussed in the next chapter.

*Maintain the chain of custody **(where).***

Another task for the CIRT is to maintain the chain of custody of the incident evidence collected. The location of the evidence from the moment it was collected to the moment it is presented in court needs to be traceable (Mandia et al. 2003). Chain-of-custody validation is one way in which a court can verify the authenticity of electronic evidence. Items to be documented include (Brezinski and Killalea 2002):

- Where, when, and by whom was the evidence collected?
- Where, when, and by whom was the evidence handled or analyzed?
- Who had custody during what period of time? How was evidence stored?
- If evidence changed custody, document when and how the transfer of custody occurred. Include all shipping information.

## 4.7 Preparing a Response Toolkit

***When** and **why** is a response toolkit necessary? **Where** is it used?*

A response toolkit is no different from the bag of tools an emergency medical responder carries or the bag a parent carries on an airplane when traveling with a young child. The toolkit prepares one for when an emergency occurs. Specifically, the incident response

toolkit will help acquire evidence and protect it from contamination. It is a mobile toolkit to be used wherever the problem occurs, and it is contained on mobile media such as disks or USB drives. Being prepared—that is, having all of the tools needed to deal with a breach—will reduce the damage and downtime in the organization as well as the efficiency and effectiveness of the investigation.

***How** is the toolkit assembled?*

The toolkit is assembled with tools that are needed in an incident including both hardware and software. Some of the software tools are system utilities (netstat, mkdir, find, etc.), and some tools are needed to analyze data such as EnCase or FTK. The toolkit needs to have the system utilities that are already on the machine because some hackers will install their own versions of system utilities (e.g., installing a new mkdir that contains malware) on your system. This fact stresses the importance of having forensically sound (in good condition) tools available in an emergency.

*Acquire necessary software to respond to incidents. Acquire necessary hardware to respond to incidents **(what).***

Carlton and Worthley have demonstrated the importance of preparing a response toolkit (2009). They collected data from both computer forensic examiners and attorneys with computer forensic experience and determined that one of the top data acquisition tasks agreed upon by both was "wiping target disk drives and verifying target disk drives are wiped." Thus, some of the main software tools besides system utilities needed in the toolkit are tools that will image the drive (e.g., dd, EnCase, etc.) and will be able to analyze/search the data (e.g., EnCase, FTK, Paraben, etc.).

Carlton and Worthley's results also showed agreement on the following tasks:

- Prepare and verify toolkit to ensure that equipment is fully functional.
- Test forensic software tools.
- Prepare and verify toolkit to ensure that all necessary hardware connectors and adapters are fully stocked.

*Acquire necessary documentation to respond to incidents **(what).***

Documentation needs to be standardized to ensure that all necessary items are recorded. Of the top twenty six data acquisition tasks that resulted from Carlton and Worthley's work, ten involved documenting specific portions of the investigation. NIST (2012) suggests utilizing an issue tracking system to document the following:

- Status of the incident
- Incident summary

- Any indicators related to the incident
- All actions taken by any incident handlers
- Chain of custody
- Impact on the organization
- Contact information for all stakeholders
- A list of all evidence acquired during the investigation
- Comments
- Next steps

There are many variations of incident forms available on the web. Figure 4.6 shows an example incident response form to be filled out when reporting an incident.

## 4.8 Training

***Why** is it important to educate the users? **Who** will do the training? How often and where should the training occur **(when) (where)?***

W. Edwards Deming, an electrical engineer well known for his management teachings and philosophy and most famous for his creation of 14 points to facilitate the improvement of processes, systems, products, and services, encouraged "training on the job." This was point number 6 of the famous 14. His point was that training is required to be able to know and understand the new skills that are required to do a job. Thus, the security strategy of all companies needs to include a *user training* layer in addition to firewalls and intrusion detection, etc. because no single person or team is responsible for the security of an organization. Everyone needs to play a role in protecting the critical assets and, furthermore, everyone is a weakness. As a matter of fact, a major security issue an enterprise faces is precarious user behavior. For example, ask a group of people what they would do if they found a USB drive in the parking lot. Most likely, at least one of them will tell you that he or she would insert the drive into a computer to determine the owner, consequently failing the penetration test. A penetration test is a method to evaluate the security of a system or network by exploiting a vulnerability. The found USB drive should be treated like a used tissue on the ground because both probably carry a virus. In another penetration test example, Symantec placed 50 smartphones around five major cities and discovered that when people found the mobile phones they accessed

**Computer Security Incident Report**

Date and time:
Location:
Status:

| **Response lead:** | **Reported by:** |
|---|---|
| Name: | Name: |
| Job title: | Job title: |
| Phone : | Phone : |
| Mobile: | Mobile: |
| Email: | Email: |

**Type of incident**

| | |
|---|---|
| ☐ Exposing confidential/classified/unclassified data | ☐ Fraud |
| ☐ Denial of service | ☐ Destroying data |
| ☐ Malware | ☐ Unauthorized use |
| ☐ Unauthorized access | ☐ Other |

Comments:

**Description of incident**

Date/time: Date: _____ Time: _____
Has the attack ended? ☐ Yes ☐ No
Duration of attack (in hours): ___
Severity of attack: ☐ Low ☐ Med ☐ High

**Actions taken**

Identification measures:
Containment measures:
Evidence collected:
Eradication measures:
Summary of incident:
Cause of incident:
Damage of incident:

**Postmortem**

What worked well:

Lessons learned:

Procedure corrections that would have improved recovery efforts:

**FIGURE 4.6**
Incident response template.

the users' sensitive corporate data, contact information, cloud-based documents, social networking, passwords, salary information, and online banking (Vance 2012). It is really a wake-up call for employers to train their employees to use strong passwords for certain applications and a PIN to unlock the phone. In addition, the stolen/found mobile phones are also being sold on black markets with each credential recovered off the phone an added bonus in the amount the phone is worth. In these examples, the weakness is the user, indicating that security training needs to be renewed. Penetration testing reminds me of the Russian proverb that Ronald Reagan made famous: **"Trust but verify."** You may trust your employees but the training and penetration testing will help to verify they know the right thing to do if confronted by a situation that could put the security of your business at risk.

Security training can be accomplished via off-site training, in-house classroom training, security-awareness websites, pushing out tips at start-up, periodically e-mailing security tips, or decorating the office with various safety reminder posters (SANS Institute 2009). There is obviously no guarantee that training will remove the problem of users clicking on an infected attachment or giving away their passwords, but training needs to be part of a comprehensive security profile to reduce the risk.

*Educate users about proper use and malware. Use lessons learned, penetration testing, and live testing* ***(how) (what).***

Users should be informed about the appropriate use of networks, hosts, and the applications they use. Training should also include guidance about malware incident prevention, which can mitigate malware incidents (Brownlee and Guttman 1998). This goal can be accomplished by sharing "lessons learned" from previous incidents so that they can see how their actions could affect the organization (Stoneburner et al. 2002). As described earlier, training can also be a result of penetration testing. Another example of a penetration test is to send inappropriate "test" e-mails to employees with the goal of education. For example, one could simulate a phishing/social engineering attack by sending out an e-mail asking users for their username and password to see how many would actually send that information back.

In addition to understanding appropriate use, users should know how to contact the response team as well as understand the services they provide. The Network Working Group suggests publishing a clear statement of the policies and procedures of the response team in order for the users to understand how to report incidents and what to expect after an incident is reported (Zimmerman and Glavach 2011).

The IT staff also needs to be trained to be able to maintain the hosts, networks, and applications in accordance with the security standards of the organization (Mandia et al. 2003). One training option is *live testing.* An example of live testing could entail simulating a cyber security incident and evaluating the reaction and processes of the incident response team. This technique is often used in educational settings.

The following is a simplified view of the *priority 1* recommendations by NIST for the **awareness and training baseline:**

| | Impact Level | | |
|---|---|---|---|
| **Control Name** | **Low** | **Moderate** | **High** |
| Formal documentation to facilitate the implementation of the security awareness and training policy and procedure | ✓ | ✓ | ✓ |
| Provide security awareness training for new employees and when changes occur in the system | ✓ | ✓ | ✓ |
| Provide security training covering technical, physical, and personal safeguards and countermeasures required prior to access | ✓ | ✓ | ✓ |

The Top 10 Ways to Shut Down the No-Tech Hacker

1. ***Go undercover:*** Be a little paranoid. Some hackers are looking for the company logo on your PC while you are working at the coffee shop, or waiting for you to discuss company secrets at the lunch hangout near your office. So cover up the company logos and keep the conversation light.
2. ***Shred everything:*** Some laws require the proper disposal of private information (HIPAA). There are people that may look through your trash hunting for personal information as well. If you do not have a shredder, you can use scissors, burn the documents outside in an open area, or submerge papers in water overnight.
3. ***Get decent locks:*** Install or use the locks that the professionals recommend—the locks that cannot be tampered with easily. It is also recommended that the keys be hidden.
4. ***Put that badge away:*** If a hacker gets one look at your badge, he or she will probably have no problem duplicating it.
5. ***Check your surveillance gear:*** Install quality cameras to minimize tampering, use multiple cameras for the same view, protect the camera from physical attack with housing, and consider hidden cameras.

6. ***Shut down shoulder surfers:*** No-tech hackers also like to watch what you are working on from afar (or over your shoulder). If you are working on something sensitive, be cognizant of your angle (e.g., sit with your back against the wall). When punching in pass codes, shield with your hand. If you suspect that someone is watching, stop what you are doing, close your screen, and determine if anything sensitive was compromised.
7. ***Block tailgaters:*** This is referring to people that walk in behind you after you have been cleared for entrance. Do not let them in! Challenge people you cannot identify and/or notify security.
8. ***Clean your car:*** Stickers on your car (e.g., parking permits) and personal papers in your car give away a lot of information.
9. ***Watch your back online:*** Never enter your personal information in an instant messenger or web browser.
10. ***Beware of social engineers:*** They are eliciting sensitive information from you. See Chapter 1 for more on social engineering.

Taken from Long (2008).

## References

Brading, A. 2012. Yahoo Voices hacked, nearly half a million emails and passwords stolen. naked security.sophos.com (July 12, 2012).

Bradley, T. 2011. Pros and cons of bringing your own device to work. *PCWorld,* 12/20/11.

Brezinski, D., and Killalea, T. 2002. Guidelines for evidence collection and archiving. Network Working Group RFC 3227, February 2002.

Brownlee, N., and Guttman, E. 1998. Expectations for computer security incident response. Network Working Group RFC 2350, June 1998.

Carlton, G., and Worthley, R. 2009. An evaluation of agreement and conflict among computer forensics experts. *42nd Hawaii International Conference on System Sciences,* pp. 1–10.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. Computer security incident handling guide. NIST special publication 800-61, revision 2, August 2012.

Cluley, G. 2012. The worst passwords you could ever choose exposed by Yahoo Voices hack. Sophos nakedsecurity.sophos.com (July 13, 2012).

Cox, A. 2012. Stalking the kill chain: The attacker's chain. RSA FirstWatch, August 16, 2012.

Cyber-Ark. 2012. 2012 Trust, security & passwords survey (http://www.websecure.com.au/blog/2012/06/cyber-ark-2012-trust-security-and-passwords-survey).

Dale, M. 2010. Secret of English muffin "nooks & crannies" is safe for now. *USA Today,* July 29, 2010.

DeFranco, J., and Laplante, P. 2011. Preparing for incident response using the Zachman framework. *IA Newsletter* 14 (3).

Grance, T., Kent, K., and Kim, B. 2004. Computer security incident handling guide. National Institute of Standards and Technology, special publication 800-61, http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf (retrieved January 19, 2010).

Grimes, R. 2010. How advanced persistent threats bypass your network security. *InfoWorld,* October 19, 2010.

———. 2012. 5 signs you've been hit with an advanced persistent threat. *InfoWorld,* October 16, 2012.

Hassell, J. 2012. 7 Tips for establishing a successful BYOD policy. *CIO Magazine,* May 17, 2012.

Leong, R. 2006. FORZA—Digital forensics investigation framework that incorporates legal issues. *Digital Investigation* 3S:29–36.

Lewis and Roca, LLP. 2011. Protecting "nooks and crannies" *Bimbo Bakeries USA, INC. V. Chris Botticella,* http://www.lrlaw.com/ipblog/blog.aspx?entry=260 (retrieved January 14, 2013).

Long, J. 2008. *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing.* Burlington, MA: Syngress Press.

Mandia, K., Prosise, C., and Pepe, M. 2003. *Incident response & computer forensics,* 2nd ed. New York: McGraw–Hill.

Mell, P., Kent, K., and Nusbaum, J. 2005. Guide to malware incident prevention and handling. NIST special publication SP800-83, November 2005.

National Security Agency. 2009. Manageable network plan.

NTT. 2009. Communications white paper, 8 elements of complete vulnerability management. September 2009.

Ponemon Institute. 2012. Cost of cyber crime study: United States" http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (retrieved January 10, 2013).

SANS Institute. 2009. The importance of security awareness training, http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013 (retrieved January 20, 2013).

Scarfone, K. and Mell, P. 2007. Guide to intrusion detection and prevention systems. NIST special publication 800-94.

Sophos. 2013. Security threat report 2013, http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx (retrieved January 9, 2013).

Souppaya, M., and Scarfone, K. 2012. Guidelines for managing and securing mobile devices in the enterprise. NIST special publication 800-124, July 2012.

Stoneburner, G., Goguen, A., and Feringa, A. 2002. Risk management guide for information technology systems. NIST special publication 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (retrieved on January 23, 2010).

Vance, A. 2012. Data security: Most finders of lost smartphones are snoops. *Bloomberg Businessweek,* March 8, 2012.

Zachman, J. 1987. A framework for information systems architecture. *IBM Systems Journal* 26 (3): 276–292.

Zhang, X., Li, C., and Zheng, W. 2004. Intrusion prevention system design. The 4th International Conference on Computer and Information Technology.

Zimmerman, S., and Glavach, D. 2011. Cyber forensics in the cloud. *IA Newsletter* 14 (1).

# 5

# *Incident Response and Digital Forensics*

Efficiency is doing things right; effectiveness is doing the right things.

**—Peter F. Drucker**

## 5.1 Introduction

Incident response (IR) and digital forensics (DF) need both efficiency and effectiveness because if they are not done correctly, your efforts will be futile. In this chapter, the fundamental processes for incident response and digital forensic analysis will be discussed. Just today, an *incident* occurred on my laptop, no less. Similarly to every other day, I dock my laptop upon my arrival and start checking my e-mail. Within a few minutes, the IT admin is at my door and announces that we have a problem. He said he received a message from the main IT office—over 300 miles away and monitoring over 20 locations and thousands of computers—that my laptop has been compromised. He was instructed to remove it from the network and begin the analysis process by scanning it for any personal information that may have been accessed by a hacker. This is a great example of an incident; as small as it sounds, it is, in fact, an incident. The official definition of an incident is a situation that has compromised the integrity, confidentiality, or availability of an enterprise network, host, or data. Other incident examples include attempting to gain unauthorized access to a system, a DDOS (distributed denial of service) attack, unauthorized use of a system, website defacement, etc.

Generally, the IR process is to detect, contain, and eradicate the incident, and the DF process is to collect, analyze, and report the evidence. In other words, once the incident is contained and eradicated, the DF professional begins the evidence collection process. The goal of the analysis is to determine (1) what happened so that reoccurrence of the incident can be avoided, and (2) whether this is a criminal case.

The cases where electronic evidence is critical are not always action packed with computer break-ins, SQL (structured query language) injections, DDOS, malware, phishing attempts, or company web page defacement. Some cases requiring electronic evidence are disloyal employees who are suspected of

industrial espionage,* breached contracts, an employee dismissal dispute, theft of company documents, inappropriate use of company resources (e.g., possession of pornography), copyright infringement (music illegally traded over the Internet), harassment (e-mail-based stalking), and identity theft.

## 5.2 Incident Response

Be prepared. We have all heard that before—especially if you were a Boy Scout or if you read the preceding chapter. This is true of life in general as well. For example, financial experts tell us to prepare for job loss by having three to six months of savings available. In a poor economy, we should have more, but the point is that we are taught to prepare for that rainy day. When an incident occurs on your system, it may be more of a hurricane. If you are prepared and monitor anything that could impede success, when something unplanned occurs, you are prepared to deal with the issue in order to get your system back up. It is like being the only house with a generator after the hurricane caused a neighborhood power loss.

The National Institute of Standards and Technology (NIST) has provided a baseline for **incident response**. Here is the simplified view of the *priority 1* recommendations. The first control (creating documentation of the IR policy and procedures) and the last control (creating an IR plan) are part of preparing for incident response, which were addressed in Chapter 4. The other controls listed will be addressed in this chapter.

Incident response is a life cycle of stages shown in Figure 5.1. We covered *preparation* in the last chapter (e.g., establishing the computer incident response team [CIRT], training the users, and installing the necessary hardware and software). The next stage, *detection/identification,* is more difficult to address because incidents are not always apparent; hence, constant monitoring (using tools acquired during the prep stage) of the assets is required to detect an

| | Impact Level | | |
|---|---|---|---|
| **Control Name** | **Low** | **Moderate** | **High** |
| Formal documentation of the IR policy and procedures | ✓ | ✓ | ✓ |
| Incident handling capability to include preparation, detection and analysis, containment, eradication, and recovery | ✓ | ✓ | ✓ |
| Implement monitoring and documentation of incidents | ✓ | ✓ | ✓ |
| Require incident reporting within a defined time period | ✓ | ✓ | ✓ |
| IR plan that is a road map for response capability and also describes the structure and organization of the IR capability | ✓ | ✓ | ✓ |

* Industrial espionage is an attempt to gain access to trade secrets.

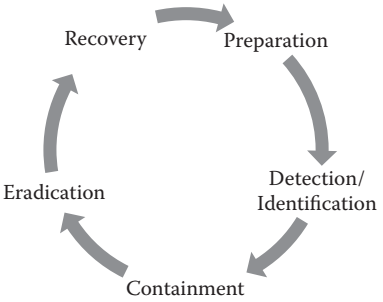



**FIGURE 5.1**
Incident response life cycle.

incident. If an anomaly is detected, the situation is analyzed to confirm that an incident is occurring. If the incident is confirmed, it needs to be *contained* (so as not to infect other parts of the system) and *eradicated*. And, finally, the *recovery* process will bring the system back to working order.

### 5.2.1 Detection/Identification

In this stage, the monitoring has produced an inconsistency or alarm that needs to be investigated to determine if an incident actually occurred. Incidents may also be discovered by a system administrator or even an end user. In any case, the first step is to verify that the "incident" is not actually an error. For example, a user error, a system/software configuration, or a hardware failure could present itself as an incident. Ways to confirm an incident include analyzing the technical details such as reports and logs, interviewing any personnel who may have insight, and reviewing the access control lists of the network topology (Mandia, Prosise, and Pepe 2003).

If it is concluded upon analysis that the incident is not an error, the type of incident needs to be determined. There are two types of incidents: (1) a *precursor* that an incident is imminent, and (2) an *indicator* that the incident is occurring or has occurred (Cichonski et al. 2012). An *incident precursor,* for example, could be server entries of a vulnerability scanner, knowledge of a new mail server exploit, or a directed threat at the organization. Some possible *incident indicators* are, for example, IDPS (intrusion, detection, and prevention systems) or antivirus alerts, a logged configuration change, failed login attempts, a large quantity of bounced e-mails, or unusual network traffic. It is not an easy process to validate an incident since an alert can be a false positive. In order to perform an effective analysis when an incident occurs, NIST (2012) recommends that the following items be in place in order to determine the scope of the incident (or precursor) more efficiently:

- Have the networks and systems profiled for normal use so file integrity and changes can easily be identified.

- Understand normal behaviors of networks, systems, and applications by reviewing log entries and security alerts so that abnormalities can be easily identified.
- Create a log retention policy to determine how long log data from firewalls, IDPSs, and applications should be stored. Log data are helpful in the analysis of an incident.
- Perform event correlation between all of the available logs (e.g., firewall, IDPS, application) as they all record different aspects of the attack.
- Keep all host clocks synchronized. As was discussed in the last chapter, it is important during an investigation that all of the logs show the same time that an attack occurred.
- Maintain a knowledge base of searchable information related to incidents and the incident response process.
- Use a separate work station for web research on unusual activity.
- Run packet sniffers (configured to specified criteria) to collect additional network traffic.
- Have a strategy in place to filter the data on categories of indicators that are of high significance to the organization's situation.
- Have plan B in place. If the incident scope is larger than can be handled by your team, seek assistance from external resources.

Finally, if an incident is a reality and the containment process is started, make sure that any evidence is documented, a chain of custody of any evidence collected is maintained, and the incident is reported to the appropriate officials within a defined time period.

### 5.2.2 Containment

The goal of the containment stage is to minimize the scope and damage of the incident. The containment strategy will depend on certain aspects of the incident, such as the damage/theft of resources, the need for evidence preservation, service availability, time and resources available to implement the strategy, and duration of the solution (Cichonski et al. 2012). For example, in a DDOS attack, shown in Figure 5.2, the attacker is attempting to make the resource unavailable to the users by a sending a flood of messages from compromised computers, which the attacker is controlling, to a network. Essentially, it is more traffic than it can handle, which means it will be inaccessible to a legitimate user.

These types of attacks can bring your favorite social networking website to a standstill for hours until the attack on the website stops. One containment strategy for DDOS is filtering the traffic directed at the victim host and then locating the machines doing the attacking. This is obviously more easily said than done because there could be 300 to 400 unique IP addresses doing the

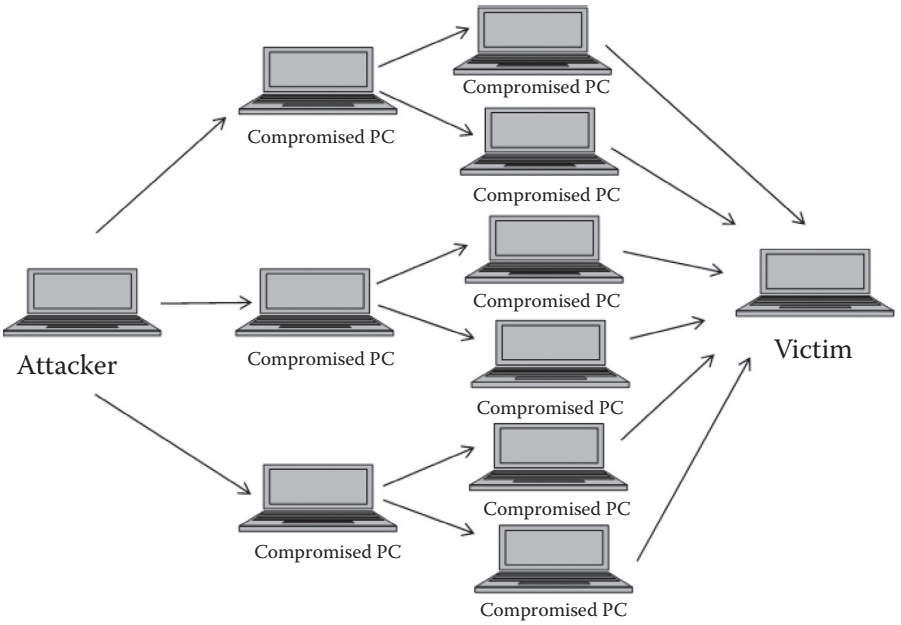



**FIGURE 5.2**
DDOS attack.

attacking. DDOS attacks are not uncommon. If you think your assets are at risk for a DDOS, then contracting with a DDOS mitigation firm—before the attack occurs, of course—may be a good idea. If you are under attack, there are DDOS mitigation firms that will help, but that is like calling on the heating, ventilation, and air conditioning service when your air conditioner does not work during a heat wave.

Containment strategies for other incidents include maintaining a low profile (so the attacker is not tipped off), avoiding potentially compromised code (recall in the last chapter that some hackers like to install their own versions of system utilities), backing up the system (in the event that evidence is needed), and changing the passwords on any of the compromised systems (FCC 2001).

### 5.2.3 Eradication

The goal of the eradication phase is to remove the cause of the incident. In addition to determining the type of attack, the containment phase hopefully provided insight into how the attack was executed—information that may help in determining an effective eradication strategy. For example, eliminating the cause of the incident may involve removing viruses or deactivating accounts that may have been breached as well as securing the vulnerability that facilitated the attack. Therefore, a clean backup to reimage

the system will be needed to ensure that malicious content is gone and that any problems cannot be spread. Then, the appropriate protection to secure the system will be implemented.

### 5.2.4 Recovery

The goal of the recovery phase is to get the system back up to normal operation. The system should also be validated. Validation means that the system is in fact operating normally after the restoration. The system should also be monitored for reinfection and for anything that was not detected originally. Once the system is back up and running, a follow-up analysis on the incident would be effective. Some aspects of the analysis should be the following (Lynch 2005):

- **Damage assessment:** Determine the systems, networks, and data affected; then identify possible remediation steps.
- **Reverse damage:** Attempt to minimize the costs associated with the incident by restoring compromised data from a backup and consulting with public relations on situations that may have had an effect on any customer base.
- **Nullify the source of the incident:** After the vulnerabilities are addressed, further incidents can be prevented through improvements to access controls.
- **Review the incident:** It is always effective to perform a postmortem on an incident to learn from any mistakes made during the response life cycle and to determine the risk level of a similar incident to other company assets.

**Example**

It is important to note that even though an incident may appear to be innocuous, you can never be too careful. This will become apparent in Chapter 7, when we go through a case study of an incident that appeared to be no big deal but was, in fact, a huge problem. That said, let us go through the IR life cycle using the laptop incident mentioned earlier in this chapter. First, the problem was *detected* by a network intrusion detection system. Once the alert from the intrusion detection system was triggered, the logs were viewed by the IT administrator. Here is an excerpt of the log from this particular incident:

```
– – – – – – – -All logs are EST– – – – – – – – - Snort Logs
= = = = = = = = = = Feb 20 09:28:56 ET TROJAN Backdoor.
Win32.Pushdo.s Checkin
[Classification: A Network Trojan was detected] {TCP}
1XX.1XX.1XX.1XX:58989 -> 213.182.5.:80 Feb 20 09:28:56 ET
TROJAN
Backdoor.Win32.Pushdo.s Chec
kin……
```

**NOTE:** Backdoor.Win32.Pushdo.s is a Trojan that allows unauthorized access and control of an affected computer.

To *contain* the incident, the laptop was immediately taken off the network (and out of my office). *Eradication* primarily consisted of removing the Trojan; however, the network traffic was also analyzed for any communication of the laptop with any malicious websites, as well as for any network vulnerabilities that were not known prior to the incident. *Recovery* consisted of patching any vulnerabilities that were determined based on log analysis, blocking the IP address of any malicious websites that were communicating with the laptop, and rebuilding the laptop by backing up personal files and reinstalling the OS, user applications, and personal files. Finally, if any personal information was compromised, those individuals would be notified.

**The Internet Crime Complaint Center (IC3)**

If you believe you are the victim of an Internet crime, or if you are aware of an attempted Internet crime, you should file a complaint with the IC3, which is an alliance between the National White Collar Crime Center and the FBI. The IC3's mission is to reduce economic crimes committed over the Internet. Internet crime is defined as:

> …any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or e-mail. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes.

The IC3 crime repository not only benefits the consumer, but also helps law enforcement to reduce Internet crime by providing training in being able to identify Internet crime issues. It is also an effective way for different law enforcement and regulatory agencies to share data.

Once a complaint is submitted, the IC3's trained analysts review and research each complaint and then disseminate the information to the appropriate federal, state, local, or international law enforcement agency. To file an Internet crime complaint, visit the IC3 website at http://www.ic3.gov.

## 5.3 Incident Response for Cloud Computing

If you are thinking about utilizing cloud computing, it is imperative that the incident response procedure of the cloud provider be understood before any

commitments are made. An organization utilizing cloud computing should consider the following in an incident response plan (Jansen and Grance 2011):

- Event data must be available in order to detect an incident. Depending on what type of cloud service is being provided (IaaS [infrastructure as a service], PaaS [platform as a service], SaaS [software as a service]), event logs may or may not be available to the customer. IaaS customers have the most access to event sources.
- The scope of the incident needs to be determined quickly. It should include a forensic copy of the incident in the event that legal proceedings are necessary.
- Containment will again depend on the cloud service provided. For example, if SaaS is the cloud service, containment may mean taking the software off-line.

Top 10 *Threat Actions* (What the Hacker Did to Cause the Breach)

1. Keylogger (spyware that captures data from user activity)
2. Guessing login credentials
3. Stolen login credentials
4. Sending data to external sites
5. Brute force and dictionary attacks (hacking by systematically using an exhaustive word list)
6. Using backdoor malware
7. Hacking the backdoor (gaining unauthorized access to a network)
8. Manipulating the security controls
9. Tampering
10. Exploiting insufficient authentication

(Taken from Verizon's 2012 Data Breach Investigations Report)

Some of those are easy fixes. Incidentally, Verizon also analyzed dates and locations of incidents and determined that hackers do most of their work Saturday through Monday and that Monday is the most productive. Good to know!

## 5.4 Digital Forensics

Crimes occur and the investigations hit a dead end because there appears to be no witness or evidence—that is, until digital forensics comes into play. The FBI solved a case using computer forensics in 2008 where a

tip was received regarding two children being sexually abused at a hotel (FBI.gov 2011). Unfortunately, by the time the tip was received, the crime had occurred. It appeared there was no evidence to charge anyone until the computer of the accused was analyzed. The evidence on the computer, a deleted e-mail with directions to the hotel where the abuse occurred, was enough to charge three adults, who are now serving life sentences in prison.

There are also times when you do not know a crime was committed until a forensic analysis is performed. Recall the situation described about the trade secret accessed by an executive after she quit and before she left to work for a competitor. The point is that an incident may appear to be innocuous or impossible to solve until the situation is analyzed. For example, in a situation where the server seemingly went off-line for no reason, after analyzing the log files, you may determine that the cause was malware installed after an intrusion. If a crime has been committed or is even suspected, it is of the utmost importance that the investigator has collected and documented the evidence in a forensically sound manner because the next step would be to hand all of the evidence off to law enforcement.

Another application for digital forensics is evidence gathering for e-discovery—the pretrial phase where electronic evidence is collected. For example, a lawyer may want to prove a spouse's infidelity and may use a forensic analysis of e-mail files to prove the accusation. In evidence gathering, technique and accuracy are critical to ensure the authenticity of the data collected when an incident occurs. The forensic investigator needs always to keep in mind that he or she may be called on to defend the techniques utilized to gather the evidence. In Chapter 6, case law is presented to demonstrate what can happen when the law is not followed while collecting and preserving evidence.

Handling digital evidence is a complex process that should be handled by a professional. If not handled with care, it can be easily destroyed and rendered inadmissible if a court case ensues. There is evidence that can be easily found but other evidence may have been hidden, deleted, or encrypted. Adding to the complexity, if the evidence is not handled properly, it will be thrown out or the case will be lost. The four main stages of the digital forensics life cycle (Figure 5.3) provide guidance for a forensic expert. The remainder of this section will review the tasks involved in each stage.

### 5.4.1 Preparation

Being prepared to perform a forensic investigation involving digital evidence will save a lot of time and effort in the long run. This includes having all of the tools and equipment needed as well as understanding how to use those tools effectively to collect and analyze the evidence. In addition, there should be a plan in place as to where the evidence will be stored securely to prevent contamination or data destruction.


**FIGURE 5.3**
Digital forensics life cycle.

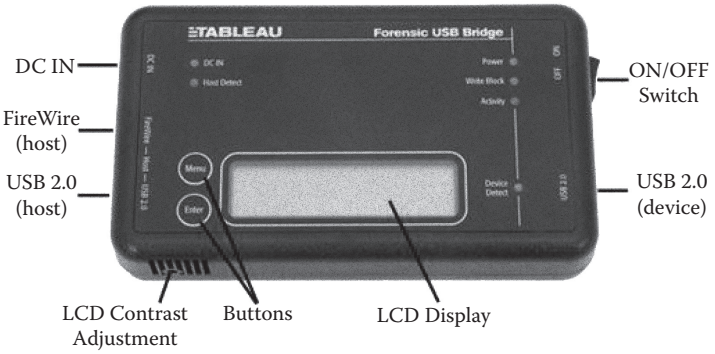



**FIGURE 5.4**
Tableau T-8 Write Blocker from Guidance Software (http://www.tableau.com).

Generally, these are the types of software and hardware needed to perform a forensic investigation: software to duplicate evidence in a forensically sound manner (that does not alter the evidence), software to analyze the drive space that was duplicated (including, at a minimum, features to identify deleted files and filter through keyword searches), and a write blocker to show that the disk copy did not modify the evidence. For example, the write blocker shown in Figure 5.4 is designed to allow forensically sound images on a USB to be extracted without fear that the data on the USB will be modified during the process.

Other items that may be useful during an investigation are notebooks, evidence bags, tape, labels, pens, cameras, antistatic bags (to transport electronic components), Faraday bags (bags to shield a device from signals that may modify evidence), and clean drives (wiped of all other data) to store the duplicated drive image. To wipe a drive, disk sanitation software* is used

* Here is an example of disk-wiping software: electronic data disposal: DOD-compliant disk sanitation software (http://www.auburn.edu/oit/it_policies/edd_dod_compliant_apps.php).

to write zeros over every bit of a drive. This is not an exhaustive list of items, but it gives you an idea of what types of things need to be considered when preparing for a digital forensic investigation.

### 5.4.2 Collection

Part of the evidence collection is to document the scene. This includes documenting things like the model and make of the devices under investigation as well as photographing the surroundings. For example, the investigator may take a photo of the screen to show what was happening when the scene was entered. In addition, the investigator may check out the task bar and take a photo of the maximized applications running. If the investigator is subpoenaed to come to court, one of the things the lawyer may do is attempt to put some doubt surrounding his or her credibility. The lawyer may ask the color of the door to the office where the computer resided. If the investigator says brown and it was dark blue, that will be strike one.

Once the scene is documented, the electronic data need to be dealt with. In responding to an incident thirty years ago, a forensic investigator would not have thought twice about the "pull the plug" method, which means shutting it down, bringing it back to a lab, and duplicating the hard drive. Due to the increase in complexity in today's computing, the investigator's response is not the same for every incident, so powering it down right away may not be in the best interest of this investigation (Note: taking it off the network is a good idea to avoid further damage.) The reason that the computer should not be turned off is that the volatile data (e.g., running processes or network connections) are lost. In addition, there is a risk that a rogue application may start a malicious attack when a shutdown is detected. Even the duplication step has changed. Not only have hard drive sizes increased considerably, but also the server that needs to be analyzed may be on the other side of the world!

I am not saying that the plug is never pulled; rather, the decision is not black and white anymore. Accordingly, there are a few ways to respond to live data collection: focusing on the *collection of the volatile data, collecting volatile data AND log files* (e.g., IDPS, router, firewall), or conducting a *full investigation by collecting everything* (a forensic duplication where every bit of data is copied). A duplication (or disk image) is necessary if court proceedings are imminent. The image is stored on an external drive, or you may send it over the network using a network utility such as netcat or cryptcat. Netcat is a networking utility that reads and writes data across a network connection. Cryptcat is Netcat with encryption. Never use the suspect system to do any analysis. Doing so will overwrite evidence.

For example, if the incident merits collecting the volatile data, the investigator may run a script from a USB drive on the suspect machine. The script will run different commands to determine the following: open ports, who is logged on to the system, dates/times, running processes, applications running on certain ports, unauthorized user accounts and privileges, etc.

Then, the script output is directed to a file stored on your USB drive. For example, a script called volatile_collection would look like this:

**E:\> volatile_collection > volatile_data_case101.txt**

*where the output from volatile_collection script would be stored in the file volatile_dat_case101.txt.*

Network data, routers, firewalls, IPDS logs, and servers may also need to be analyzed (via network logs) for anything suspicious to determine the scope of the incident, who was involved, and a timeline of events. And, finally, the investigator must identify other sources of data that could go beyond a hard drive, such as a USB drive or mobile phone.

All of this digital evidence collected must be preserved to be suitable in court. Digital evidence is very fragile, like footprints in snow or on the sand, because it is easily destroyed or changed. The FBI suggests having a secure location for storage (locked up), having sufficient backup copies (two suggested), having proof that the data have not been altered (hash algorithm), and establishing a *chain of custody,* which is a written log (a.k.a. evidence log) to document when media go in or out of storage (Cameron 2011). In order for the data to be admissible, it has to be proven that they have not been tampered with; therefore, you should be able to trace the location of the evidence from the moment it was collected to the moment it appears in court. If there is a time period that is unaccounted for, there is a chance that changes could have been made to the data. One way to preserve evidence is to transfer digital information onto a read-only, nonrewritable CD-ROM and/or uploading the data onto a secure server and hashing (discussed earlier) the file to ensure the data's integrity.

### 5.4.3 Analysis

Following data collection is data analysis. The image of the suspect machine(s) needs to be restored so that the analysis of the evidence can begin. The image should be restored on a clean (wiped) drive that is slightly larger or restored to a clean destination drive that was made by the same manufacturer to ensure that the image will fit. Next, the review process begins by using one of the forensic tools such as EnCase, (forensic toolkit) FTK, P2 by Paraben, Helix 3, etc. To recover deleted files, the unallocated space of the image needs to be reviewed. The investigator may find whole files or file fragments since files are never removed from the hard drive when the delete feature is utilized. What is deleted is the pointer the operating system used to build the directory tree structure. Once that pointer is gone, the operating system will not be able to find the file—but the investigator can! Keep in mind, however, that when new files are created, a memory spot is chosen, so there is a chance that the file is written over or at least part of the file. Here is why: All data are arranged on a hard drive into *allocation units* called *clusters.* If the data being stored require

less storage than a cluster size, the entire cluster is still reserved for that file. The unused space in that cluster is call *slack space.* There is an example in Figure 5.5.

But, deleting that 20K file frees up the space for a new file. If that cluster is chosen, the new file is going to be written on top of the old file. If the new file is smaller than 20K, then part of that 20K file will be retrievable (Figure 5.6).

Evaluating every file on the restored image can be an arduous task; thus, one trick a forensic examiner will use is identifying files with known hashed values. Known file hashes can be files that are received from a manufacturer for popular software applications. Other known hashes can be from movies, cracking tools, music files, and images. The National Software Reference Library (http://www.nsrl.nist.gov) provides values for common software applications. An investigator may be able to reduce the number of files needed to be analyzed by 90 percent by using the "hashkeeper paradigm," which assumes that similar files produce the same hash value (Mares 2002):

1. Obtain a list of hash values of "known" files.
2. Obtain the hashes of the suspect files.
3. Compare the two hash lists to match the known files or identify the unknown files.
4. Eliminate the "known" files from the search.
5. Identify and review the unknown files.

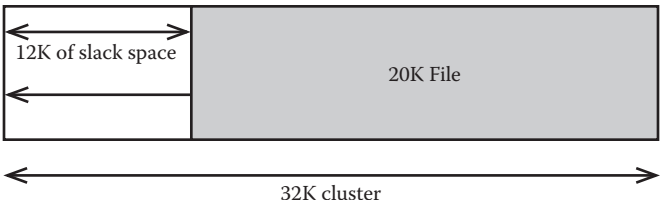



**FIGURE 5.5**
Slack space.

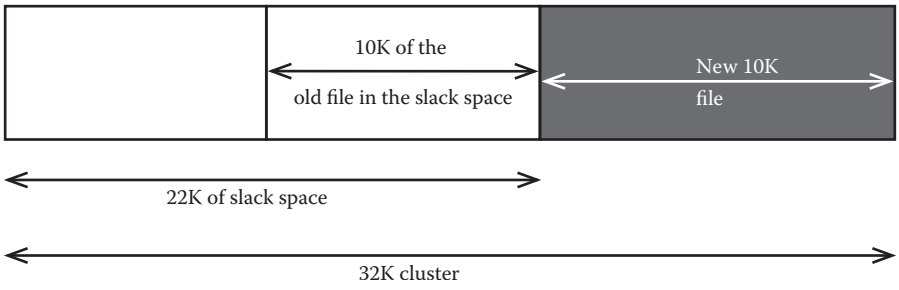



**FIGURE 5.6**
Slack space with a partial file.

For string searches within the data, the drive needs to have all compressed files decompressed and all encrypted files unencrypted. Then, just as you do with web searches, you should use effective key words to pare down results. The exact search methodology used depends on the forensic software tool you are using, what you are the looking for (e.g., files, web browser history, or e-mails), the format of the data, your time constraints, and whether the suspect is aware of the investigation. If so, he or she may have deleted some files.

A common investigation is an Internet usage analysis that monitors inappropriate usage at work where, for example, an employee is gambling or viewing pornography. Divorce lawyers may use this type of analysis to prove infidelity by showing evidence on a social networking site or proving a spouse was on a blog website looking for advice on how to get an easy divorce. An anonymous blog posting can be attributed to a spouse by showing that he or she made purchases with a credit card before and/or after the post on the blog. Web browsers store multiple pieces of information, such as history of pages visited, recently typed URLs, cached versions of previously viewed pages, and favorites. The challenge is also in showing that the accused was actually the one using that computer at the time of the incident. For example, if pornography was viewed on a particular employee's computer, the investigator has to make sure that employee was not on vacation or in meetings all day when the abuse occurred.

When doing this type of analysis (aka a *temporal analysis*), the investigator may want to reconstruct the web page. The web page can be reconstructed by searching the index.dat file for files that are associated with a given URL. Then, the investigator can look for those files in the cache and copy them to a temporary directory. The reconstructed page should be viewed in a browser that is off-line so that the browser does not access the Internet. If the reconstructed page accesses the Internet, it may follow the URL and download the latest version of the page from the server and will not be the version of the web page that the suspect viewed at the time of the incident. Note that the presence of a single image file does not indicate that the individual visited a website. Because there are times when images are a result of a pop-up or redirect, it is important that the investigator also determine which sites were visited prior to the site in question. Recall the case of Julie Amero discussed at the beginning of Chapter 2. These are just a few of the many techniques an investigator could utilize for an effective and forensically sound Internet usage analysis.

E-mail analysis is also very common. The investigator may be tasked to prove a certain policy violation, harassment, or impersonation. It may be as simple as finding the e-mail and determining who sent it and who received it, or as complicated as reconstructing the entire e-mail chain. This is also an analysis that should be done off-line so that no e-mails are sent or received inadvertently during the analysis.

### 5.4.4 Reporting

The final stage in the digital forensics life cycle is reporting the results of the analysis in the previous stage as well as describing reasoning behind actions, tool choices, and procedures. NIST (2006) describes three main factors that affect reporting: *alternative explanations, audience consideration,* and *actionable information.*

*Alternative explanations* back up the conclusions of the incident by including all plausible explanations for what happened. In the Julie Amero case, she was convicted (later overturned) of viewing pornography on a school computer in front of minors. Had the investigators looked for alternative explanations, they would have figured out that the pornography websites viewed were caused by spyware. Instead, the clearly ignorant original investigators misled the jury by only presenting evidence in the temporary Internet files directory and the school firewall logs showing that pornography websites were accessed. They missed the alternative explanation and caused her to be unfairly convicted because their findings (temporary Internet files and firewall logs) do not demonstrate a user's intent. Upon reanalysis by expert forensic investigators (Eckelberry et al. 2007), it was discovered that the antivirus software was an out-of-date trial version, that there was no antispyware* software installed on the system, and that the spyware was definitely installed prior to the incident.

The original investigators also misled the jury by informing them that spyware is not capable of spawning pop-ups (not true), that pop-ups cannot be in an endless loop (not true), and that the red *link* color used for some of the text on the porn website (that they showed the jury) indicated Amero clicked on the links (the link visits, whether intentional or not, are shown in the visited color, which they indicated was red). In this particular case, the link was red; however, if the original investigators had opened the browser preferences, they would have noted a few things: (1) The links were selected to be green if a site was visited, and (2) the html source code changed the font color to red. The investigators also misled the jury by telling them that the only way spyware is installed on a computer is by actually visiting a pornographic site (not true). Eckelberry et al. (2007) determined that this particular spyware was installed right after a Halloween screen saver was downloaded. There were multiple inconsistencies with the original investigation. I encourage you to read this case as it illustrates very clearly what NOT to do in a forensic investigation.

Reports on the results of a forensics analysis will vary in content and detail based on the incident. Just as in any writing, *audience consideration* is important. Thus, the level of detail of a forensic analysis report is determined by the audience who needs the report. If the analysis resulted in a noncriminal case, the executives or management may want a simple overview

* Antispyware is software designed to detect and remove a malicious application from a computer.

of the incident, how it was resolved, and how another occurrence will be prevented. A system administrator may need details regarding network traffic. Or, if it is criminal case, law enforcement will require a very detailed report. In all cases, the report should be accurate, concise, and complete. Nelson, Phillips, and Steuart (2010) suggest that the report should include supporting material, an explanation of the examination and data collection methods, calculations (e.g., MD5 hash), an explanation of any uncertainty and possible errors, and an explanation of the results found and references utilized for the content of the report.

The third report factor is *actionable information*, where the information provided may lead to another source of information and/or information that will help to prevent future similar incidents.

Another type of report is an *after action report* that, in addition to identifying issues that need to be improved upon for future incidents, may also include improvements to the team or process. For example, team members may decide to improve their skills using the forensic software, fix the acceptable-use policy for the organization, or modify the incident response procedure. This will, of course, help in staying current with the changes in law, technology, and the latest cyber issues.

### A Great Example of Security through Obscurity* (and Digital Forensics)

If you have an e-mail account that you think is anonymous, think again. An anonymous e-mail account is an account that is created without revealing any personal information. However, that alone does not guarantee anonymity. An anonymous e-mail account, when used with mail clients such as Outlook, appends the IP address information to each e-mail's metadata† that are sent—which is a great clue for a forensic investigator. Therefore, if the e-mails are investigated, the IP address can help pinpoint the sender. You may be wondering who is looking at your e-mail. Due to the provisions of 1986's Stored Communications Act (SCA), the government can access e-mails stored by a third-party service provider. However, there are a few caveats to that access. If the e-mail is in "electronic storage" AND less than 180 days old, a warrant needs to be obtained to access the e-mails. E-mails not in "electronic storage" OR in "electronic storage" more than 180 days can be accessed with a subpoena. Electronic storage is defined as e-mail that has been received by the Internet service provider (ISP) but has not been opened by the recipient (Jarrett et al. 2009).

* Security through obscurity is a derogatory term that implies that secrecy or hiding something makes it secure. It is similar to when I put my laptop on the front seat of my car and cover it by a blanket while parked in a public parking lot. If it is discovered, there is nothing really protecting it from getting stolen.

† Metadata are data that describe other data.

The way to make your Internet and e-mail activity really anonymous is to use software such as Tor,* which conceals a user's location even if the e-mails are accessed. This type of software is often used by journalists, the military, and activists to protect research, investigations, etc. Hence, Tor needs to be running in order to make an anonymous e-mail account actually anonymous. Unfortunately for a recent CIA director and his girlfriend, this software was not used and their extramarital affair was revealed by piecing together the e-mail trail left by the girlfriend—even though anonymous e-mail accounts were utilized by both of them.

The investigation began due to harassing e-mails sent to another woman (Perez, Gorman, and Barrett 2012). The FBI analyzed the logs from the e-mail provider to determine who sent the harassing e-mails. They specifically looked at the metadata from the e-mails to determine the locations from which the e-mails were sent. By comparing the e-mail metadata from the e-mail providers, guest lists from hotels, and IP login records (hotel WiFi), the FBI put the puzzle together and discovered the identity of the sender of the harassing e-mails as well as her affair with the CIA director (Isikoff and Sullivan 2012). This discovery led to the CIA director's resignation.

## 5.5 Mobile Phone Forensics

Mobile phone forensics is the science of recovering digital evidence from a mobile phone. Mobile phones, being much more than a communication tool, retain a substantial amount of data: calendars, photos, call logs, text messages, web history, etc. The cellular network also retains data regarding location. Mobile phone data have helped convict many criminals. A man was convicted of the murder of a college student with the help of cellular phone network data (Summers 2003). The killer was actually helping the police locate the college student by showing them around the college campus. At the same time, the police were analyzing the cellular network data. When the victim's phone was turned off, it disengaged itself from a specific cellular tower near the killer's home; due to the mounting evidence, the killer eventually admitted to the crime.

Mobile phone forensics uses the digital forensics life cycle just described. The challenge with mobile phone forensics is the frequent release of new phone models, often making cables and accessories obsolete, as well as the

* Tor (https://www.torproject.org/) is software that was developed originally to protect government communication. Now it is used by people as a safeguard to their privacy (not anonymity). It is used to safeguard a person's behavior and interests. One of the examples on the Tor website is when traveling abroad, Tor can hide your connection to your employer's computer so that your national origin is not revealed.

lack of a standard for where mobile phones store messages. The upside is that the puzzle can be more easily solved because of all of the information stored on cell phones: calls (incoming, outgoing, missed), address books, texts, e-mail, chat, Internet use, photos, videos, calendars, music, voice records, notes—the list could go on forever with all the apps available as well.

A brief overview of NIST (2007) recommendations to seize mobile phones in an investigation will be presented in this section. For further details, please download the special publication listed in the reference section of this chapter. First, consider all of the types of evidence needed from the phone. For example, if fingerprints are needed, follow the appropriate handling procedures for acquiring fingerprints. The investigator may also want to record any viewable information from the phone. It is advisable to leave the phone off for two reasons: First, there is a potential for data loss if the battery dies and, second, data may be overwritten if network activity occurs. If the phone must remain on for some reason, the phone should be placed in a container that blocks radio frequency or in airplane mode. Finally, that container should be placed into a labeled evidence bag that is then sealed to restrict access. Before leaving the scene, collect all related phone hardware such as cradles, cables, manuals, and packaging—anything you find related to the phone.

To collect the evidence from the mobile phone, NIST (2007) also recommends isolating the phone from all other devices used for data synchronization. Imaging the device at the scene is the best option if battery depletion is an issue. If not, bring it back to a lab to acquire the data. There are many memory categories as well as various memory structures that vary among manufacturers. Sometimes it is just call log data, so it may not be necessary to recover all of the data on the phone. If you are not familiar with acquiring data from a particular phone, it is best to seek assistance from another digital forensic professional.

**InfraGard**

A great organization for security professionals is InfraGard—a not-for-profit organization that is a partnership between the private sector and the Federal Bureau of Investigation (FBI). The members of InfraGard are individuals from businesses, academic institutions, state and local law enforcement, and any person that wants to participate in sharing information and intelligence that may prevent hostile acts against the United States (http://www.infragard.net). For example, a university professor (and his class) helped the FBI catch criminals involved in a case called "Trident Breach." In this case, the criminals infected computers (via an e-mail link or attachment) with the ZeuS virus, which is essentially a key logger application that logged the user's banking information. Then, the criminals were able to lure other people (aka money mules) into "work-at-home" schemes where their "job" was completing banking transactions.

The banking transaction went as follows: The mule opened the bank account, the money was deposited from the ZeuS-infected computer user's account into the mule's account, and then the mule withdrew the cash and sent it to the criminals. Gary Warner, professor at the University of Alabama at Birmingham (and member of InfraGard), used data-mining techniques to establish the links between the ZeuS-infected computers and the origin of the mass infector. Most of the hackers and the "mules" were caught. The 18 mules still at large were found by his students using computer forensic investigation techniques such as crawling social networking sights to identify the remaining suspects (Engel 2012).

To apply for membership to InfraGard, fill out the online application (http://www.infragard.net/member.php), read and sign the "Rules of Behavior" form, and submit. Once you are accepted, find your local chapter and attend any meetings of interest.

## References

Cameron, S. 2011. Digital evidence. *FBI Law Enforcement Bulletin,* August 2011.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. Computer security incident handling guide. NIST special publication 800-61, revision 2.

Eckelberry, A., Dardick, G., Folkerts, J., Shipp, A., Sites, E., Stewart, J., and Stuart, R. 2007. Technical review of the trial testimony *State of Connecticut v. Julie Amero.* March 21, 2007, http://www.sunbelt-software.com/ihs/alex/julieamerosummary.pdf (retrieved March 2, 2013).

Engel, R. 2012. University professor helps FBI crack $70 million cybercrime ring. http://rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring (retrieved August 3, 2012).

FBI.gov. 2011. Regional labs help solve local crimes, 5/31/11, http://www.fbi.gov/news/stories/2011/may/forensics_053111 (retrieved February 9, 2013).

FCC (Federal Communications Commission). 2001. FCC computer security incident response guide.

Isikoff, M., and Sullivan, B. 2012. Emails on "coming and goings" of Petraeus, other military officials escalated FBI concerns. NBC News, November 12, 2012. http://openchannel.nbcnews.com/_news/2012/11/12/15119872-emails-on-coming-and-goings-of-petraeus-other-military-officials-escalated-fbi-concerns?lite (retrieved March 8, 2013).

Jansen, W., and Ayers, R. 2007. Guidelines on cell phone forensics. NIST special publication 800-101.

Jansen, W., and Grance, T. 2011. Guidelines on security and privacy in public cloud computing. NIST special publication 800-144.

Jarrett, H., Bailie, M., Hagen, E., and Judish, N. 2009. Searching and seizing computers and obtaining electronic evidence in criminal investigations. US Department of Justice. http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (retrieved March 12, 2013).

Kent, K., Chevalier, S., Grance, T., and Dang, H. 2006. Guide to integrating forensic techniques into incident response. NIST special publication 800-86, August 2006.

Lynch, W. 2005. Writing an incident handling and recovery plan. http://www.net-security.org/article.php?id=775&p=3 (retrieved February 21, 2013).

Mandia, K., Prosise, C., and Pepe, M. 2003. *Incident response & computer forensics,* 2nd ed. New York: McGraw–Hill.

Mares, D. 2002. Using file hashes to reduce forensic analysis. *SC Magazine,* May 2002.

Nelson, B., Phillips, A., and Steuart, C. 2010. *Guide to computer forensics and investigations,* 4E. Boston: Cengage Learning, Course Technology.

Perez, E., Gorman, S., and Barrett, D. 2012. FBI scrutinized on Petraeus. *Wall Street Journal,* November 12, 2012.

Summers, C. 2003. Mobile phones—The new fingerprints. BBC News, December 18, 2003.

Verizon. 2012. 2012 Data breach investigations report. http://www.indefenseofdata.com/data-breach-trends-stats/ (retrieved February 8, 2013).

# 6

# *The Law*

> It takes 20 years to build a reputation and five minutes to ruin it. If you think about that you'll do things differently.
>
> **—Warren Buffett**

## 6.1 Introduction

Technology has positively influenced our world in many innovative ways: medicine, aviation, education, business, engineering, and, as an added bonus, a smartphone can tell you how long the wait is for your favorite ride at Disney. However, technology obviously has spawned many negative side effects discussed in this book. It is safe to say that with every technological advancement comes a new vulnerability that a hacker can exploit. In addition, this rapid advancement causes gaps with security compliance rules, digital evidence handling, and the law. In this chapter, you will be introduced to the prevalent compliance standards, evidence rules, laws for acquiring evidence, case law, and e-discovery. These are all topics security professionals need to understand to do their job effectively.

## 6.2 Compliance

Compliance is a major concern for the chief security officers (CSOs) of today. This refers to implementing a specific legislation related to the type of data your company collects, accesses, stores, and transmits. For the most part, the legislation affects the way in which data are handled to help maximize confidentiality. Hence, this directly affects the ways in which security professionals do their jobs as these laws are essentially standards that require the implementation of technology in a way that facilitates the security of sensitive data. In this section, I will present an overview of the technology requirements of a few of the security laws, regulations, and guidelines.

### 6.2.1 The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA addresses safeguarding electronically protected healthcare information (EPHI). EPHI includes information that a business *creates, receives, maintains,* or *transmits.* EPHI "must be protected against reasonable anticipated threats, hazards, and impermissible uses or disclosures" (Scholl et al. 2008). The entities that need to follow HIPAA (healthcare providers, health plans, healthcare clearinghouses, and Medicare prescription drug sponsors) need to ensure that the security triad (confidentiality, integrity, and availability) of the electronic healthcare information is maintained. The HIPAA standards outlined in the National Institute of Standards and Technology (NIST) special publication 800-66 present all of the considerations when applying the HIPAA security rule: administrative safeguards, physical safeguards, technical safeguards, organizational requirements, policies and procedures, and documentation requirements. The following list contains ten steps to HIPAA security (Kibbe 2005):

1. Understand the importance of computer security.
2. Make sure the entire organization understands the seriousness of securing EPHI.
3. Catalog all the information system components that interact with EPHI.
4. Prepare so that the security triad is ensured. Do not wait for the disaster.
5. Secure your network.
6. Update antivirus protection.
7. Consider which communication needs to be encrypted.
8. Consider the "chain of trust"* between business partners (insurance companies, billing services, hospitals, labs, and ISPs).
9. Demand that your vendors (products and services used) understand HIPAA.
10. Have a plan with your goals and needs in mind.

### 6.2.2 The Payment Card Industry Data Security Standard (PCI-DSS)

The goal of PCI-DSS is to optimize the security of debit and credit card transactions by reducing fraud and protecting the personal identity information of the card holders. The PCI Security Standards Council is responsible for maintaining the PCI security standards. The PCI-DSS applies to any entity that is involved in payment card processing. The "high-level overview" provided by PCI is as follows (PCI Security Standards Council 2010):

* "Chain of trust" is a term referring to the fact that each entity sharing the EPHI has the necessary security protections to ensure the HIPAA requirements.

1. Build and maintain a secure network by installing and maintaining an effective firewall configuration to protect cardholder data. Use strong passwords and other security parameters.
2. Protect cardholder data by encrypting the transmission of cardholder data.
3. Maintain a vulnerability management program by updating antivirus software and maintaining secure systems and applications.
4. Implement strong access control to cardholder data and use a unique ID for each person accessing cardholder information.
5. Regularly monitor and test network resources and cardholder data. Conduct regularly scheduled vulnerability and penetration tests of systems and processes.
6. Maintain an information security policy to address information security for all personnel.

A study done by the Ponemon Institute (2011) of 670 US and multinational IT and IT security practitioners involved in their organizations' PCI compliance efforts revealed that organizations compliant with PCI-DSS have reduced their overall cardholder data breaches. The survey looked at many facets of payment security to determine the benefit of the PCI-DSS compliance efforts. Most important, the survey results illustrate that the benefit of compliance is that the organizations that fully comply decrease their chances of incidents. Specifically, 38 percent of organizations that were PCI-DSS- *fully compliant* and 78 percent of organizations that were PCI-DSS-*noncompliant* experienced two or more incidents from 2009 to 2011.

### 6.2.3 The North American Electric Reliability Corporation-Critical Infrastructure Protection Committee (NERC-CIP)

The power grid, part of our critical infrastructure, is a target for hackers. NERC is responsible for establishing security standards for the power grid to ensure the most reliable system possible. NERC's critical infrastructure protection (CIP) standards and guidelines are applied to improve the reliability of the physical (equipment and control centers) and cyber (hardware and software) security of the bulk power systems in North America. The standards, which follow, address the vulnerabilities and risks of bulk electric systems (BESs). Details for each standard are available on the NERC website (http://www.nerc.com):

- **CIP 002: Critical Cyber Asset Identification**—Use risk-based assessment to identify assets.
- **CIP 003: Security Management Controls**—Access control to critical cyber assets.

- **CIP 004: Personnel and Training**—Require personnel risk assessment, training, and security awareness.
- **CIP 005: Electronic Security Perimeter**—Manage perimeters surrounding BES cyber systems.
- **CIP 006: Physical Security for Critical Cyber Assets**—Create and maintain tools and procedures to monitor access points to perimeters.
- **CIP 007: Systems Security Management**—Develop processes and procedures to secure critical and noncritical cyber assets.
- **CIP 008: Incident Reporting and Response Planning**—Maintain a cyber security incident response strategy.
- **CIP 009: Recovery Plans for Critical Cyber Assets**—Create a recovery plan to restore critical cyber assets.

### 6.2.4 The Gramm-Leach-Bliley Act (GLBA)

The GLBA is a federal law that governs how financial institutions treat consumer private personal information. The main components of the GLBA are the *Financial Privacy Rule, Safeguards Rule,* and *Pretexting Protection.* The *Financial Privacy Rule* requires that there are precautions implemented that ensure that customer personal information remains secure and confidential. Interestingly, the American retailer Victoria's Secret is one of the reasons privacy protections were implemented in the GLBA. Congressman Joe Barton from Texas was concerned that his credit union sold his address to Victoria's Secret, so he started receiving the catalog at his Washington address (Hoofnagle and Honig 2005):

> This was troubling—he didn't want his wife thinking that he bought lingerie for women in Washington, or that he spent his time browsing through such material. Barton explained that he maintained an account in Washington for incidental expenses, but used it very little. Neither he nor his wife had purchased anything from Victoria's Secret at the Washington address. Barton smelled a skunk; he reasoned that since he spent so little money in Washington, his credit union was the only business with his address.

The *Safeguards Rule* refers to the tools a security program requires to protect customer information. This would include any safeguard needed to acquire, access, process, store, and distribute the information. The Federal Trade Commission (FTC) suggests that all areas of operation that deal with customer information need to be secured, especially employee management and training, information systems, and detecting and managing system failures. Many of the techniques mentioned in Chapter 3 are utilized in the implementation of the safeguards rule. For example, it recommends

closely evaluating, training, and implementing access control techniques for employees that are facilitating the security plan.

The *Pretexting Protection* refers to protecting against social engineering tactics. As was discussed in Chapter 1, social engineering preys on the weakness of the human actor. It is a scheme to acquire personal information by impersonation or fraudulent activities. Basic suggestions to avoid these social engineering tactics are never to give out personal information unless you know the person or have initiated the contact AND training employees about spear phishing and e-mail vulnerabilities.

### 6.2.5 Sarbanes-Oxley Act (SOX)

SOX is a federal law that improves the accuracy and reliability of financial reporting to prevent accounting fraud. There are two sections of the law that apply directly to information security: Section 302, "Corporate Responsibility for Financial Reports," and Section 404, "Management Assessment of Internal Controls" (SANS Institute 2004). Section 302 states that the CEO and CFO must certify that financial reports are accurate. Section 404 states that, in addition to assessing the effectiveness of the internal controls, the assessment must be evaluated by an outside auditor. Since the reporting systems are based on technology and need to be secure, a portion of the implementation of SOX compliance is done by the information security team. Here are some of the elements of a secure plan for SOX compliance (George 2011):

1. Implement secure sockets layer (SSL) encryption for sensitive data for web-enabled applications.
2. Utilize end-point protection such as antivirus and malware protection; intrusion, detection, and prevention systems (IDPS); and firewalls.
3. Mitigate the operation attack surface on all systems accessing financial systems (e.g., install software updates, check for system vulnerabilities, etc.).
4. For access to financial systems, consider application streaming or desktop virtualization as it can protect critical applications from hackers.
5. Monitor activity of the databases containing sensitive information.

### 6.2.6 The Federal Information Security Management Act (FISMA)

FISMA is part of the E-Government Act, which addresses the improvement of the information security effort as it affects the economic and national security interests of the United States. FISMA requires all federal agencies to "develop, document, and implement an agency-wide program to provide information security for the information and information systems that

support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source" (Scholl et al. 2012). The recommended security controls from NIST, discussed throughout this book, were developed in response to FISMA. For further information, please see the publicly preferred available NIST special publication 800-53.

## 6.3 Laws for Acquiring Evidence

Whether you are law enforcement or the digital forensics professional, it is important to know the laws for acquiring evidence. If the laws are not followed, someone's innocence cannot be proven or a criminal will continue to walk the streets. Unfortunately, knowing the laws is not enough. One needs to be familiar with the status of particular laws within the jurisdiction of where the crime occurred as well. For example, warrants to search cell phones are part of a recent debate. If law enforcement seizes and searches a cell phone without a warrant and finds an incriminating text on it, that evidence may or may not be admissible because of the Fourth Amendment to the US Constitution, which states that the right of the people

> …to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

In a California case, *People v. Diaz,* the suspect was arrested following an illegal drug transaction. The police seized his cell phone and searched it at the police station after the suspect denied the charges. The police found an incriminating text message on his cell phone. The message was "6 4 80," which translates to "six pills for $80.00." The suspect confessed, but later attempted to suppress the text message evidence, citing the Fourth Amendment's protection from unreasonable search and seizure. This motion was denied because the court decided that the cell phone was considered property incidental to a person and therefore searchable without a warrant (Minkevitch 2011). In a Texas case, *United States v. Finley,* there was a similar ruling where an arrest occurred when the suspect was caught selling drugs. Again, incriminating text messages were found on the suspect's cell phone and the court allowed the cell phone evidence and did not report a Fourth Amendment violation. The court compared reading the cell phone texts to retrieving call records from a pager seized at an arrest (pager searching is allowed). It is also significant that the cell phone was found on the suspect's person at the time of the arrest.

Conversely, in a Colorado case, *People v. Schutter,* text message evidence acquired without a search warrant was suppressed due to the Fourth Amendment. The defendant left his phone in a convenience store restroom and the clerk was too busy to open the restroom when the defendant returned to retrieve the phone. The defendant left the store, and the phone was later given to the police to search in order to determine its owner. In that cell phone search, the police found incriminating evidence that suggested the phone's owner was selling illegal drugs. At the hearing, the cell phone evidence was suppressed by the district court. It was suppressed because the police "violated the defendant's reasonable expectation of privacy." If the phone had been "abandoned, lost, or mislaid," the search would have fallen under a "community-caretaking exception" and the evidence may not have been suppressed.

The Fourth Amendment is again a factor in a case involving the death of a six-year-old boy. While the police were at the home of the murder suspect, they found a cell phone that had this unsent text message: *"Wat if I got 2 take him 2 da hospital wat do I say and dos marks on his neck omg."* There were also other text messages that pointed to the suspect harming the child, yet the court suppressed this evidence as it violated the Fourth Amendment. This is an ongoing case whose ruling will likely be appealed (Masnick 2012). The point is that until the US Supreme Court decides under which circumstances an officer may search the contents of a cell phone, members of law enforcement need to be aware of the laws in their jurisdiction (Kruger 2013).

The **USA Provide Appropriate Tools Required to Intercept and Obstruct Terrorism** (USA PATRIOT*) Act was enacted as a result of the terrorist attacks on September 11, 2001. The PATRIOT Act covers many areas to help law enforcement to improve counterterrorism efforts (www.justice.gov). Portions of the Act were intended to update the law to reflect new technologies and threats. For example, Section 220 allows law enforcement to deal with search warrants more easily. Nationwide warrants for e-mail can be issued instead of a search warrant for each jurisdiction where the e-mail may be located. For example, a warrant would be issued for the ISP location rather than where the crime was committed. The PATRIOT Act also considers computer hacking the same as physical trespassing. Now, hacking victims can seek assistance from law enforcement. In Sections 202 and 217, the PATRIOT Act permits intercepting electronic communications of "computer trespassers" (Smith et al. 2002).

Another law that affects digital forensics is the **Electronic Communications Privacy Act** of 1986 (ECPA†). The ECPA replaced the Wiretap Act of 1968, which was written to address intercepting communication using traditional telephones. The ECPA focuses on communications and stored e-mail.

* For further information on the PATRIOT Act, see Smith, M. S. et al., 2002, the CRS Report for Congress, http://epic.org/privacy/terrorism/usapatriot/RL31289.pdf.

† The information for ECPA came from the US Department of Justice (http://www.it.ojp.gov/).

The main goal of the ECPA was to ease restrictions for law enforcement when attempting to obtain stored communications. The ECPA has three titles:

1. Title I, the **Wiretap Act,** prohibits obtaining communications as evidence illegally. A warrant (good for thirty days) is required to intercept communications. Probable cause needs to be shown to have a warrant issued. There is also an exception for operators and service providers if it is part of employment.
2. Title II, the **Stored Communications Act** (SCA), protects the privacy of the contents of files stored by a service provider.
3. Title III, the **Pen Register Act,** requires the government to obtain a court order if it needs to install and use a pen register or a trap-and-trace to investigate criminal activity. A pen register is a device that captures outgoing (dialed) call information. A trap-and-trace is a device that captures incoming call information. The call information is related to the number dialed—not actual communications.

Interpreting legislation is not that simple. According to the SCA, "electronic storage" is defined as electronic communication that has been received but not opened by the recipient. That is pretty straightforward, but, "electronic storage" is also defined as communication that has been opened and is stored by the ISP for backup protection (Jarrett et al. 2009). So the question is, if e-mail is opened AND is not downloaded (remains at the ISP) to an e-mail client (e.g., Outlook), is it there for backup purposes? OR did the recipient just choose not to use an e-mail client? If the e-mail is older than 180 days or opened, "electronic storage" does not matter. If the e-mail is less than 180 days old AND in storage, then it is considered in "electronic storage," which means that accessing it without a search warrant violates the SCA.

In the divorce case *Jennings v. Jennings,* the husband admitted he was having an affair. The wife told her daughter-in-law, who decided to "help" by hacking into the husband's personal e-mail account. She guessed at the answers to the security questions, changed his password, and began her detective work. The daughter-in-law printed out the e-mails between the husband and his mistress and gave them to the wife and the wife's attorney and private investigator. The husband learned of the hack in the court proceedings. He then sued the daughter-in-law civilly for violating the SCA (by accessing his e-mail). The circuit court granted judgment in favor of the daughter-in-law, stating that the e-mails were not in electronic storage (they were opened), so it was not a violation of the SCA to access them. The appeals court reversed that judgment, stating that the e-mails WERE in electronic storage (because they were left on the Yahoo! server for backup purposes) and thus covered by the SCA. Then, it was reversed AGAIN by the South Carolina Supreme Court as they did not agree that leaving the e-mails on the Yahoo! server

indicated that the e-mails were in storage. The final judgment was that the e-mails were already opened by the recipient but not deleted and therefore NOT in "electronic storage." This means that those e-mails could be accessed by unauthorized third parties without violation of the SCA (Cedarbaum et al. 2012). The e-mail storage debate may be something that the US Supreme Court will resolve.

Many of these laws refer to the need of a warrant. The exception to the warrant requirement is called the **Plain View Doctrine.** Officers are able to seize evidence not listed on the warrant while they are present in an area that is protected by the Fourth Amendment (e.g., someone's home) if the items found are in "plain view." Plain view factors are defined as follows: The officer already has a warrant, the officer is in the Fourth Amendment-protected area, the item to be seized is in plain view, and the item is immediately recognized by the officer as evidence of the crime without needing to make any further intrusion (Ryan 2013). Here are two examples:

*In plain view:* ***Horton v. California,*** 496 U.S.128 (1990).* An officer had a search warrant to search Horton's home for the proceeds of a robbery. In his search, he did not find the stolen property, but he found weapons in plain view and seized them. This evidence was not suppressed, and Horton was convicted of robbery. The appeals court agreed that the evidence was in plain view, since it was immediately recognized to be part of the robbery.

*Not in plain view:* ***Minnesota v. Dickerson,*** 508 U.S. 366, 375 (1993).† An officer observed a man (Dickerson) coming out of a building known for cocaine traffic. He was walking toward the police officer and abruptly changed direction once he noticed the police officer. The officer followed him into an alley and ordered him to stop and submit to a pat-down search. The search did not reveal any weapons, but the officer was suspicious of something he felt in the suspect's jacket. The officer put his fingers into the jacket pocket and determined it was a lump of crack cocaine. Dickerson was arrested for possession of a controlled substance. Dickerson moved to suppress the cocaine evidence since it was not found under "plain view." The suppression appeal failed as the officer was justified in frisking Dickerson to determine if he had any weapons, and the analogy was made that sense of touch is a reliable perception and no different from plain view. This was reversed by the Minnesota Court of Appeals, which stated that the pat-down search was lawful, but that the officer crossed the line by reaching in Dickerson's pocket

* The details of this case can be found on Justia.com US Supreme Court Center (http://supreme.justia.com/cases/federal/us/496/128/case.html).

† The details of this case can be found on the Cornell University Law School website (http://www.law.cornell.edu/supct/html/91-2019.ZO.html).

when he determined the item he felt was not a weapon. Thus, the cocaine was NOT in plain view. I will present examples of the plain view doctrine as it applies to digital forensics later in the case law section.

## 6.4 Evidence Rules

A person will encounter many hurdles when going to court with digital evidence. This is because digital evidence is volatile and can be modified very easily; thus, there is uncertainty that needs to be resolved when presenting digital evidence in court. For any evidence to be admitted, it needs to follow the Federal Rules of Evidence (FRE). The focus for digital evidence is on the "best evidence rule" (FRE 1002—requirement of the original): "To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."

As the original may be a challenge when dealing with digital evidence, the FRE addresses this in its definition of "original" (FRE 1001 (3)):

> An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

In *Doe v. US*,* the plaintiff received blood transfusions from 22 donors in 1985. In 1988, John Doe tested positive for HIV. The case alleged that the 1985 transfusions caused John Doe's HIV virus. The defendant sought to have HIV database records admitted as evidence in this case. The plaintiff contested the validity of the database records and argued that they "violated the best evidence rule, are hearsay,† and are unreliable." The court overruled the best evidence objection because an accurate printout is acceptable as evidence.

Other challenges a prosecutor may encounter are *adverse inference* and *spoliation*. *Adverse inference* is when someone either did not produce evidence or spoiled the evidence to exclude it from the case. As an example, a computer was confiscated from an individual accused of stealing information. During the analysis of the computer, it was discovered that the evidence was deleted

* *Doe v. US* case details: http://www.leagle.com/xmlResult.aspx?page=3&xmldoc=19922318805FSupp1513_12132.xml&docbase=CSLWAR2-1986-2006&SizeDisp=7.

† Hearsay is a statement made while testifying where the information was from another person. This is not admissible evidence.

because it would have had a detrimental effect on the defense side of the case. The *spoliation* of evidence also includes situations where the evidence was damaged, whether intentionally or not. These situations can be detected by a forensic examiner finding evidence of disk wiping on the confiscated device.

## 6.5 E-discovery

"Discovery" is a legal term describing the request of information from one party involved in a lawsuit to the opposing party. Electronic "discovery" (e-discovery) is when the request is made for electronic artifacts in a lawsuit, such as word processing documents, spreadsheets, e-mails, audio, and/or video. E-discovery differs from the digital forensic request in that e-discovery is acquiring *readily accessible* documents on the storage device. Digital forensics analysis goes deeper because the information acquired is from *not* readily accessible data as that could be encrypted, deleted, damaged, in the slack pace, web search activity, or in the form of metadata. For example, Figure 6.1 shows Google search information that could have been acquired by the forensic professionals in the *Casey Anthony* trial to show malice intent by the defendant prior to the disappearance of her daughter. Web search activity is not readily available information and therefore would not be part of an e-discovery request. Analyzing web activity is a digital forensic activity because there is much more analysis required. For example, the information in Figure 6.1 does not exactly show intent of the defendant


**FIGURE 6.1**
Google Search evidence acquired in Casey Anthony trial provided by Jones Dykstra & Associates, Inc. (http://www.jonesdykstra.com/)

unless data are acquired that show who was *using* the computer at the time the "neck-breaking" search was done. Information to support the claim that the defendant was using the computer could include data showing logins to websites visited before and after the web search.

Another difference between e-discovery and digital forensics is that the e-discovery artifacts are usually handed over to the legal team to analyze, whereas the digital forensic results are usually analyzed by the digital forensic professionals and then reported to the legal team. E-discovery can also be a very expensive request since the amount of available electronic information is vast. For example, in the 2010 case where Oracle sued Google for copyright infringement (claiming that the Google Android operating system violated Oracle's Java patents and copyrights), the key piece of evidence was an e-mail that was part of the e-discovery request. The e-mail was written by a Google engineer and read: *"We conclude that we need to negotiate a license for Java under the terms we need."*

That e-mail may have implied that Google *also* thought it needed a license. Imagine how many documents had to be analyzed to find that *one* e-mail? Did you imagine 97 million documents? Indeed, the Oracle e-discovery request to Google resulted in collecting over 97 million documents from over 86 custodians. Ultimately, the verdict was "not proven,"* but Google spent over $4 million† in e-discovery, experts, and other court fees. Google then sued Oracle for the entire $4 million, but only the costs for the experts and other fees were granted.‡ In the end, Oracle was ordered to pay $1.13 million of Google's court expenses, but nothing for e-discovery (Brodkin 2012).

There have been cases where e-discovery costs for the defendant were partially covered by the plaintiff. In *Lubber Inc. v. Optari*,§ the verdict was that both parties had to share the e-discovery material production cost. Essentially, the court recognized that the requesting party may think twice about discovery requests if it has to pay part of the cost to produce the material. In the end, the court's reasoning for not granting the e-discovery cost to Google was that "the problem with Google's e-discovery bill of costs is that many of item-line descriptions seemingly bill for 'intellectual effort' such as organizing, searching, and analyzing the discovery documents."†

---

* *Oracle America, Inc. v. Google Inc.*, jury's special verdict form, case 3:10-CV-03561-WHA, filed May 23, 2012, https://www.docketalarm.com/cases/California_Northern_District_Court/3--10-cv-03561/Oracle_America_Inc_v_Google_Inc/1190/

† Google Inc.'s bill of costs, case no. 3:10-CV-03561, http://docs.justia.com/cases/federal/district-courts/california/candce/3:2010cv03561/231846/1216/0.pdf?ts=1341576301

‡ Order regarding bill of costs, case no. C 10-03561, http://docs.justia.com/cases/federal/district-courts/california/candce/3:2010cv03561/231846/1241/0.pdf?ts=1346833638

§ http://www.applieddiscovery.com/ws_display.asp?filter=Case%20Summaries%20Detail&item_id={2381A663-573A-4712-AF03-681D2AA3566B}

## 6.6 Case Law

Case law refers to a body of writings explaining court rulings in different cases. Generally, they are used by judges as precedents when making decisions or by lawyers as persuasive material when they are researching or presenting their case. For instance, in the *Oracle v. Google* case, a few cases were used to support Oracle NOT paying Google's e-discovery bill, such as:

- *Parrish v. Manatt, Phelps & Phillips, LLP*[*]: The court stated, "The reproduction costs defendants incurred in collecting, reviewing, and preparing client documents for production were necessary expenditures made for the purpose of advancing the investigation and discovery phase of the action." In other words, these were normal requests and thus the defendants need to pay.
- *Service Emp. Int'l Union v. Rosselli*[†]: The plaintiff's objections to deposition-related costs were overruled.
- *Petroliam Nasional Berhad v. GoDaddy.com, Inc*[‡]: Costs were "necessary to convert data into a readable format" as they were essential in reproducing formal documents that were used in the case.

It is important for a digital forensics professional to be aware of case law as it aids in effectively reaching your goal. In the case of *US v. Carey*, Mr. Carey was under investigation for selling and possessing cocaine. The search warrant allowed the police to search the defendant's computer files for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." During the search, the detective found child pornography. Even though the files had sexually suggestive names, the detective said that, until he opened each file (he opened 95 of them), he did not know its contents. By opening up the additional files after discovering the first sexually explicit file, the detective exceeded the scope of the warrant. Thus, the search was now "unconstitutional." Therefore, the evidence was not admissible under the *plain view doctrine* because the contents of the files were not inadvertently discovered. In a similar situation, *US v. Gray*, the FBI had a search warrant to search Gray's computer for hacking evidence. The agent came upon child pornography and suspended the search until

[*] http://docs.justia.com/cases/federal/district-courts/california/candce/3:2010cv03200/229842/100/0.pdf?ts=1302595391

[†] http://docs.justia.com/cases/federal/district-courts/california/candce/3:2009cv00404/210971/837/0.pdf?ts=1288681162

[‡] http://scholar.google.com/scholar_case?case=3382396509643399226&q=Petroliam+Nasional+Berhad+v.+GoDaddy.com&hl=en&as_sdt=2,5&as_vis=1

a second warrant was obtained in which she could lawfully search for the sexually explicit material on the computer. In this case, the evidence was admissible.

## References

Brodkin, J. 2012. Oracle must pay Google $1M to cover costs in failed patent case. *Ars technica,* September 5, 2012. http://arstechnica.com/tech-policy/2012/09/oracle-must-pay-google-1m-to-cover-costs-in-failed-patent-case/ (retrieved 3/15/13).

Cedarbaum, J., Jain, S., Zachary, H., Powell, B., and Gorelick, J. 2012. United States: South Carolina *Jennings* decision deepens divide over scope of Stored Communications Act, October 23, 2012. http://www.mondaq.com (retrieved April 6, 2013).

George, R. 2011. 10 Best practices for meeting SOX security requirements. *InformationWeek Security,* December 15, 2011. http://www.informationweek.com/security/management/10-tips-for-sarbanes-oxley-compliance/232300585 (retrieved April 2, 2013).

Hoofnagle, C. J., and Honig, E. 2005. Victoria's secret and financial privacy. Electronic Privacy Information Center, http://epic.org/privacy/glba/victoriassecret.html (retrieved April 2, 2013).

Jarrett, H., Bailie, M., Hagen, E., and Judish, N. 2009. Searching and seizing computers and obtaining electronic evidence in criminal investigations. US Department of Justice. http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (retrieved March 12, 2013).

Kibbe, D. C. 2005. Ten steps to HIPAA security compliance. *Family Practice Management* 12 (4): 43–49.

Kruger, K. 2013. Warrantless searches of cellphones: Is the law clearly established? *The Police Chief,* March 2013, http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2431&issue_id=72011 (retrieved March 24, 2013).

Masnick, M. 2012. Murder case upended after police read phone texts without a warrant, September 6, 2012. http://www.techdirt.com/articles/20120905/17595720288/murder-case-upended-after-police-read-phone-texts-without-warrant.shtml (retrieved April 5, 2013).

Minkevitch, H. 2011. *People v. Diaz:* Is your iPhone constitutionally protected? *Berkeley Technology Law Journal* (http://btlj.org/2011/02/23/people-v-diaz-is-your-iphone-constitutionally-protected/).

PCI (Payment Card Industry) Security Standards Council. 2010. Data security standard, "requirements and security assessment procedures, version 2.0. https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (retrieved March 29, 2013).

Ponemon Institute. 2011. 2011 PCI-DSS compliance trends study: Survey of IT & IT security practitioners in the U.S.

Ryan, J. 2013. Plain view doctrine. http://policelink.monster.com/training/articles/2043-plain-view-doctrine- (retrieved April 6, 2013).

SANS Institute. 2004. An overview of Sarbanes-Oxley for the information security professional. www.SANS.com (retrieved April 2, 2013).

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., and Steinberg, D. 2008. An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. NIST special publication 800-66, http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (retrieved July 18, 2012).

Smith, M., Seifert, J., McLoughlin, G., and Moteff, J. 2002. CRS report for Congress. The Internet and the USA Patriot Act: Potential implications for electronic privacy, security, commerce, and government, March 4, 2002. http://epic.org/privacy/terrorism/usapatriot/RL31289.pdf (retrieved March 6, 2013).

# 7

# *Theory to Practice*

> Many of life's failures are people who did not realize how close they were to success when they gave up.
>
> **—Thomas Edison**

## 7.1 Introduction

It is time to put the concepts you have been reading about into practice. The previous chapters gave you the foundation needed to understand the implications of decisions made during real security incidents. There are three cases presented in this chapter. I will present the first two cases in a story format as they happened. The third case recounts the details of a high-profile litigation. After each case, an *after action report* (aka a postmortem) will be presented. A postmortem is an exercise that a team performs to review a project with the goal that improvements will be made for the next project. Organizations that want to learn from their mistakes and continuously improve do this type of exercise after a challenging project. It is important to note that this is also a great exercise to do when a project is successful so that things that worked well are repeated. Since the presentation in this chapter is for illustrative purposes, the postmortems have been pared down a bit. If you are interested in learning the complete process to perform a postmortem, read "An Approach to Postmorta, Postparta and Post Project Reviews" by Norman Kerth.

## 7.2 Case Study 1: It Is All Fun and Games until Something Gets Deleted*

You are the new chief information security officer (CISO) of a large organization. As with most senior-level executives, you are responsible for maintaining and overseeing many moving pieces in the organization; however,

* This is a fictional case based on the experiences of Robert Maley, founder of Strategic CISO and a former CISO of a large organization.

since you have only been in place a few days, you are still getting a grasp on the organization as a whole. You are still determining the critical assets, the topology of the network, and, most important, the personnel resources you have to help you do your job of securing the infrastructure of this company. Unfortunately, you have already noticed that industry best practices in the area of security have not found their way to this organization … yet.

You begin your day like any other day with meetings and e-mail. It is about 11:00 a.m., and you decide to take a break. You stop in the restroom and overhear a conversation between an engineer and the IT administrator who walked in after you; they are discussing a recent incident. Here is what you hear:

*Paul (engineer):* Hey, David, how's it going?
*David (IT administrator):* Pretty good, Paul. Sorry I didn't meet you guys last night for happy hour. I noticed at the end of the day that the web server went offline.
*Paul:* Oh, did you get it back up and running?
*David:* Yeah, it was no big deal. The global.asa* file was deleted. We got it back up and running in no time.
*Paul:* That's cool. I'll let you know when we plan another happy hour.

You are alarmed at the casual conversation regarding this incident. You leave the restroom and wait for David in the hall, who realizes you overheard the conversation when he sees you:

*CISO:* Hey, David. I overheard your conversation about the web server issue. I would like to review the incident report.
*David (now looks like a deer caught in the headlights):* I didn't fill out a report because it was an easy fix.
*CISO:* Let's discuss this in my office.

Before you give David a lecture on why documenting an incident and following an incident response process is crucial, you decide to listen to the facts first. You begin your discussion in line with the *incident response* process:

*CISO:* David, please first explain in detail how you detected this incident.
*David:* Sure. I uploaded a new PDF to the database and wanted to test how the information from the PDF was displayed on our website, but I couldn't access the website because it was offline. I checked the root directory of the server and noticed the global.asa file was

* The global.asa file is a special file that handles session and applications events on a server. In this case, the main function of the globa.asa file is to provide information to the web page regarding where the information that needs to be displayed is located.

> missing. I looked in the log file and determined the global.asa file was deleted yesterday, which in effect "breaks" the website. When I looked around a little more on the server, I noticed that a lot of game and movie files had been uploaded. I figured someone just uploaded them to play a game or watch a movie because I did an antivirus scan and didn't see any evidence of someone remotely controlling the server.* Before I did anything else, I called Tim on the Network Security Team to keep him informed. He suggested searching for more malware in the form of spyware and Trojan infections. When nothing was discovered, the network security team declared this was not a hack, and thus not an incident. So, I started recovering the system by deleting the movies and games and uploading the backup of the global.asa file.

At this point, David feels confident about his explanation because he followed the correct process by calling the Network Security Team and performing the actions prescribed by the team. The only thing he is a little worried about is whether the CISO is going to question why the pirated movies were not reported to law enforcement, so he decides to clarify before the CISO says anything: "We didn't report the incident regarding the movies because we couldn't afford to have our server taken offline. Law enforcement would have needed to review the server for evidence, right?"

You are silent for a few minutes. There is so much to do here, so you ignore his last statement for now and think about their process. You are thinking that David did go through the IR process: he *detected* the incident, *contained* and *eradicated* the incident by deleting the games and movies, and *recovered* the web server by restoring the missing file. However, the analysis was clearly lacking in thoroughness, which caused a premature declaration that this was not a hack. You break the silence with the million dollar question: "You didn't determine how the games and movies were uploaded. Did you check the server logs? If the vulnerability is still there, you didn't solve the problem!" David starts to sweat. He is really not to blame; he was following the advice of the security team. However, before David can answer, you say, "David, please get Tim and let's meet in the conference room in ten minutes."

You go straight to the conference room and wait. David and Tim arrive and sit down. You start the conversation:

*CISO:* Tim, David has brought me up to date with this incident. I am concerned about the lack of thoroughness in the investigation

* By "remotely controlling the server," David is referring to the server being part of a botnet. This was discussed in Chapter 1. It is important to note that not all botnets can be detected with antivirus software. One may need a specific application that specifically removes that type of malicious software. Therefore, just because David did not find it with antivirus software does not mean that there was not any malicious software on the system.

process being utilized, but we can work on that after we resolve the current issue. First, we need to determine the vulnerability that allowed the uploads so that it can be eliminated. What is the status of the last vulnerability scan?

*Tim:* I am not sure when the last scan was performed. I will get back to you after I look at the logs that we do have from the intrusion detection system and check some of the access control mechanisms.

*CISO:* David, I want you to document what has occurred so far and also work with Tim to document the rest of the investigation. Please keep me informed.

After three hours go by, David appears in your doorway and says:

> I have an update. Tim used a forensic tool to evaluate the server over the wire. With this tool, he was able to connect to the server and *collect* the information needed for analysis in a proper forensic manner. He determined that the vulnerability was that the FTP account was configured without a password. When he *analyzed* the data in the log files, he found that malware was in fact introduced to the web server. However, the games and movies were not uploaded onto the server using the open FTP account. They were uploaded via a back door—the second vulnerability. We suspect now that our server was being utilized as a peer-to-peer (P2P*) mechanism.

You contain your urge to gloat and say, "So, a rootkit† was introduced through the FTP account and the games and movies were introduced though a back door access created by the rootkit. If I am correct, the games will be reinstalled shortly since the recovery performed yesterday did not include elimination of these vulnerabilities." David looks a little deflated because you stole his punch line. David continues, "Yes, the games and movies were in fact reinstalled after I deleted them last night, so you are correct."

David gets a call from Tim:

*David:* Hi, Tim. Yes, I am in his office.

David puts the phone on speaker and Tim says,

> Hi, everyone, here is the update: Upon analysis of the log files, we determined that the hacker deleted the global.asa file yesterday. It appears

* P2P is a network where users can connect to each other and share files.

† A rootkit is a type of software that can enable privileged access such as back door into a system. The back door is a way to access a system in a way that the site administrator never intended.

> that this hacker was cleaning up unneeded files on the server, probably to make room for additional movies and games so that he wouldn't get noticed. During that process, he accidentally deleted the global.asa file. It also appears that, according to the log file, there were 500 individual downloads last week alone. So, I just deleted the rootkit and secured the FTP account, which should mitigate any further issues. The worst part of this incident is that, according to the log files, our server has been compromised for a year.

You tell them both that they did a great job, but they are not finished. Tim now needs to pass the evidence of this intrusion to law enforcement for further analysis as they may be able to determine the identity of the criminal. Tomorrow, you will break the news about ramping up their incident response process as well as explain how this incident could have easily been avoided.

### 7.2.1 After Action Report

#### *7.2.1.1 What Worked Well?*

The most obvious thing this organization did well was to hire a CISO, since it is clear it needed a leader to implement security best practices into its operations. For example, the company had the right tools, but did not use them effectively. There was intrusion detection, but the parameters were set so liberally that hardly any events were logged. A vulnerability scanner had been installed, but it was not configured properly. Before the CISO came onboard, this organization was getting hit with virus after virus, so the CISO was tasked to create a security posture for the company.

#### *7.2.1.2 Lessons Learned*

Even though you have the right tools, training is needed to use them effectively. For example, although the company had a vulnerability scanner, a daily or even weekly vulnerability scan would have showed the open FTP account early on. Not everyone needs a daily vulnerability scan. The asset value will determine the frequency and thoroughness of your scanning because each scan requires resources. Someone has to review the vulnerability report!

Have an incident response team in place. The network security team's first priority is not incident response; therefore, they were not prepared to investigate this incident. It was clear that their goal was to get the server back up and running. The incident response team will also make sure the organization is prepared for an incident and has a process in place to handle one.

#### *7.2.1.3 What to Do Differently Next Time*

These can also be called the after action items:

1. Make sure the intrusion detection system has current signature files. Signature files will help the system recognize known malicious threats. This is similar to the way in which antivirus applications detect malware.
2. Migrate into an enterprise server format where the technical controls would be more rigorous. In other words, the company needs a centralized server resource as opposed to having each department run its own servers. This will help the company analyze and secure the servers in a consistent manner. In addition, a company should hire people to manage that effort.
3. Implement incident response training for all of the IT administrators. This will help them recognize incidents as well as understand the importance of ensuring that the incident response process is followed.
4. Review and update the change management request process to ensure that proper access control is implemented.
5. Conduct regular vulnerability scans.

The 2012 LinkedIn database breach where hackers obtained millions upon millions of access credentials was a wake-up call to companies that have not kept a close enough eye on their organization's security plan. Here are nine techniques that a CISO can employ to improve the effectiveness of an organization's security posture (Schwartz 2012):

1. ***Deploy CISOs in advance:*** This is part of being prepared. Would you move to a town that did not have a fire department, police department, or hospital? Hire the CISO before the security breach happens—not after.
2. ***Acknowledge how CISOs reduce security costs:*** According to the Ponemon Institute (2012), the cost of data breach attacks has declined from $7.2 million to $5.5 million. In addition, they reported that the organizations that employed CISOs had an $80 cost savings per compromised record. Companies that outsourced this function only saved $41 per compromised record. The reason a CISO reduces costs is that he or she can help facilitate security best practices that have been proven successful.
3. ***Allow CISOs to help guide new technology decisions:*** The evolution of technology is ongoing. The CISO needs to be accepting of new technologies in order to factor them into the organization's overall security profile.

4. ***Make CEOs demand security posture details:*** Effective communication between the CEO and CISO is a must. In other words, the CEO needs to have an appreciation and understanding of the organization's security posture just as he or she has an appreciation and understanding of the organization's current sales.
5. ***Treat information security as a risk:*** Something as simple as a phishing attack on a company can compromise the security of critical information. The CISO needs to be well informed of all vulnerabilities in the organization as well as vulnerabilities at organizations that share any of his or her organization's computing resources.
6. ***Consider a placeholder CISO:*** If your company does not have a CISO, consider outsourcing the position to a reputable security company until the needs of the organization are determined.
7. ***Identify crown jewels:*** In part of the risk analysis, determine the value of the critical assets. In addition, risk should be reassessed periodically. For example, if a password file has doubled the number of users, increasing its protection should be a priority.
8. ***Beware of a false sense of security:*** Use a third party, who may see things that you do not, to assess the risk and security posture of the organization.
9. ***Treat advanced threats as common:*** Consider advanced persistent threats (APTs, discussed earlier) as more prevalent than ever. The standard information security defense should never be standard; it needs to evolve as the threats evolve.

## 7.3 Case Study 2: How Is This Working for You?

Let us fast-forward two years at the same organization and see how well the CISO's security plan has worked out. Over the two years, a few people have been hired for the computer incident response team (CIRT), so we have a new cast of characters in our story. We have Jenny leading the CIRT team and Alex and Justin working with her. We also still have David, who continues in his IT administrator role but has since been trained in incident response per one of the after action items in our last case study.

Another one of the changes the CISO instated was to write and enforce an acceptable use policy (AUP). We discussed AUPs in Chapter 4. One of the restrictions at this organization, according to the AUP, was that instant messaging (IM) is not allowed. It was felt that IM was a distraction to the employee and, more important, it was deemed a security risk to the network. IM tools are security risks because they can circumvent the security measures

(e.g., employee can casually send out confidential information) of the organization as well as become a conduit for worms* and viruses.

The exact AUP excerpt read as follows:

> INSTANT MESSAGING and CHAT Services:
> *Use of instant messaging or chat applications on the company network is not acceptable.*

To monitor the IM restriction, the intrusion detection system was configured to generate an alert if IM was being utilized. Well, one afternoon, Alex informed Jenny that the IM alarm had been triggered. Upon analysis, the identity of the employee was discovered, but the CIRT needed to analyze the hard drive to determine the nature of the messages. If the messages were inappropriate, this would be grounds for the employee's dismissal. Alex informed Jenny of the situation and they made a plan. They needed to inform the director of Human Resources (HR) of the violation and plan a time to approach the employee to confiscate the employee's hard drive. The team decided to approach the employee within the hour.

The CIRT team and director of HR gathered and approached the employee. Jenny said, "It has come to our attention that you are in violation of this organization's acceptable use policy. We will need to confiscate your hard drive." The employee obviously was stunned, but was cooperative.

The CIRT team brought the hard drive back to their lab, made a forensically sound† copy of the hard drive, and began their analysis. They knew the instant massager client, so they needed to analyze the application to determine the messages that were received and sent. They discovered that the messages were of an inappropriate nature, which is grounds for dismissal. They needed to follow appropriate procedures to store the evidence in the event that the employee decided to contest the dismissal. For now, the situation was handed over to Human Resources to dismiss the employee.

### 7.3.1 After Action Report

#### *7.3.1.1 What Worked Well?*

The CISO has done an excellent job implementing industry's best practices into this organization's security profile. An AUP policy was written, implemented, and followed. The organization had a dedicated team to respond to the incident and they followed forensically sound procedures to analyze the situation.

---

* The terms *worms* and *viruses* are often used interchangeably but are in fact different. A virus is distributed by making copies of itself. A worm uses a computer network to replicate itself. It searches for servers with security holes and makes copies of itself there.

† "Forensically sound" refers to the manner in which the electronic information was acquired. The process ensures that the acquired information is as it was originally discovered and thus reliable enough to be evidence in a court proceeding.

#### *7.3.1.2 Lessons Learned*

The importance of implementing industry best practices both to secure the company assets and to be able to respond to incidents is priceless.

#### *7.3.1.3 What to Do Differently Next Time*

Nothing! Well done!

**To Outsource or Not**

Some companies choose to outsource the security function to a third party because they can save money or the third party can do a better job for the same money. Examples of outsourced functions could be hiring consultants to help deal with a data breach or hiring them to store your data.

Outsourcing needs to be thought about carefully because your company is ultimately responsible in the case of a security breach. Conducting a risk assessment to help with that decision is necessary (Condon 2007): Determine the potential impact on the organization if a data breach occurs and determine if the outsourcing company will make your data vulnerable. According to the Ponemon Institute (2012), 41 percent of organizations had a data breach caused by a third party (outsourcers having access to protected data, cloud providers, and/or business partners). Most likely, determining the quality of service you will get from the security firm will be confirmed by references from other customers and a site visit (Burson 2010).

## 7.4 Case Study 3: The Weakest Link*

### 7.4.1 Background

Roger Duronio was dissatisfied with his yearly bonus from his employer, the financial services company, UBS-Painewebber (UBS-PW). Like many companies, after the events of nine/eleven, profits were down at UBS-PW, which affected the employee bonus program. On February 22, 2002, the bonuses were distributed. Duronio's bonus was $15,000 less (his compensation for the year would be $160,000 instead of $175,000) than what he expected, even

* The information from this case was provided by Keith J. Jones: the court indictment and articles written by Sharon Gaudin (all are referenced at the end of the chapter). Mr. Jones is owner and senior partner with Jones Dykstra & Associates, Inc. (http://www.jonesdykstra.com/). JDA is a company specializing in computer forensics, e-discovery, litigation support, and training services. He is on the board of directors of the Consortium of Digital Forensics Specialists (CDFS; developing standards for the digital forensics profession). He is also the author of *Real Digital Forensics: Computer Security and Incident Response* (2005) and *The Anti-Hacker Toolkit* (2002).

though the employees were informed previously that this bonus reduction would be happening. Duronio had a history of being dissatisfied with his pay. The prior year he had approached his boss for a raise. His boss was able to approve a $10,000 salary raise; however, the boss felt Duronio was still unsatisfied with his compensation. This was apparent when Duronio received his bonus on February 22, 2002. After receiving his bonus, he went straight to his boss and demanded the remainder be awarded. Otherwise, he would quit that very day. The boss made an attempt to have the full bonus awarded, but was not successful. When he went back to give Duronio the bad news, his boxes were already packed. His vengeful plan was already in the works.

Duronio's revenge on UBS-PW caused him to be charged with *securities fraud* (count 1), *mail fraud* (counts 2 and 3), and *fraud and related activity in connection with computers* (count 4). In the high-profile case, the US Department of Justice hired computer forensics expert Keith Jones to testify on behalf of the prosecution. The defense hired Kevin Faulkner as their forensics expert.

### 7.4.2 The Crime

On Monday, March 4, 2002, Duronio, a former systems administrator for UBS-PW, executed a logic bomb within its network that disabled nearly 2,000 of the company's servers. He planted the logic bomb prior to his exit from the company. A logic bomb is malicious code inserted into an application that will execute when the specified condition is met. His logic bomb was set to execute when the stock market opened at 9:30 a.m. EST on March 4, 2002. The code had four components:

1. **Destruction:** The server would delete all files.
2. **Distribution:** The bomb would be pushed from the central server to 370 branch offices.
3. **Persistence:** The bomb would continue to run regardless of a reboot or power down.
4. **Backup trigger:** If the logic bomb code was discovered, another code bomb would execute the destruction.

The logic bomb was only the first part of the plan. The second part of his plan was to profit from this attack. Duronio purchased 330 PUT* options ($25,000 worth) of UBS-PW shares. He was essentially betting on the fact

* A "PUT" option is purchased when someone thinks a stock will decrease in value by a certain date. In other words, it is essentially a contract between two parties to exchange an asset at a specified price by a certain date. For example, party A can purchase the stock at the decreased rate (specified in the contract) and sell it at the strike price (specified in the contract). The profit = (strike price) – (decreased rate) – (the cost of the PUT option). If the stock does not decrease in value, party A loses the cost of the PUT option.

that he would make money when the stock lost value due to his logic bomb attack. UBS-PW reported a $3 million loss* in recovery from this attack.

### 7.4.3 The Trial

Mr. Jones, the forensics expert for the prosecution, had his work cut out for him. He had to piece together the puzzle that proved the deceptive actions of Duronio as well as present the facts of the case in a way that could be understood by the jury. The forensic expert for the defense, Kevin Faulkner, had to prove the opposite. The trial went on for five weeks.

#### *7.4.3.1 The Defense*

The goal of the defense was to show that evidence presented by the prosecution was incomplete and unreliable. Their main focus was on the fact that there was no mirror image of the data and consequently no way to prove that Duronio was the attacker. In reference to the fact that there were only backup tapes of the hard disk files to analyze because a forensic image (a bit-for-bit copy) of the drive was not taken, Mr. Faulker said, "I couldn't look at all of the data." He stated, "To preserve digital evidence, a forensic image is best practice." He only had 6.5 gigabytes of data from a 30 gigabyte capacity server to analyze. The defense attorney questioning Faulkner attempted to assert that a forensic analysis of backup tapes is not sufficient to make any hard conclusions. In addition, the attorney was putting into question the chain-of-custody of the data because the backup tapes were handled by another forensics company no longer involved in the case. This former forensics company also had a reputation of hiring hackers which, in their opinion, put the integrity of the forensics company as well as the integrity of the data previously handled by hackers into question.

The defense attorney also questioned Mr. Jones about the validity of the analysis using only backup tapes of hard disk files instead of a bit-for-bit copy of the servers. Mr. Jones testified that taking an image of damaged servers would not have aided in the success of the analysis. He felt the amount of data available was sufficient to draw conclusions.

#### *7.4.3.2 The Prosecution*

Over five days, Mr. Jones testified that Duronio's actions caused the UBS-PW stock trading servers to be inoperable. He was able to extract IP address, date, and time information that connected the attacker to the specific servers and confirmed when and where the attacker had planted

* The loss included $898,780 on servers, $260,473 on investigative services, and $1,987,036 on technical consultants to help with the recovery.

the logic bomb. The IP address pointed directly to Duronio's home in all cases but one. The exception pointed to Duronio's workstation at UBS-PW. The US Secret Service also found parts of the logic bomb code on two machines within Duronio's home in addition to a hard copy printout of the code.

Mr. Faulkner pointed out the alleged holes in the prosecution's testimony. He testified that the log data in general are poor forensic evidence. The logs that were used by the prosecution were the VPN, WTMP, and SU (switch user logs show when users switch to *root* user* access). It is important to note here that root user access, which Duronio had, would be necessary to plant a logic bomb. Mr. Faulkner also provided a few other facts that attempted to put the attacker ID into question:

1. The log data are not reliable, as they can be edited by the root user.
2. The log files data would not be able to identify whether someone accessed the server using a back door.†
3. There was, in fact, back door entry to the server in question.
4. Although the time of their access was not identified to match the time of the logic bomb insert, two people (only identified via login ID) accessed the server using the back door.
5. There were two other current systems administrators who were also employed at UBS at the time of the attack who could have been the attacker. However, the two other system administrators were cleared of any suspicion of direct involvement after the first forensic investigation team (no longer working on the case) analyzed their machines. That company did find a few strings of the logic bomb code in the swap space‡ on one of the systems administrator's machines. But there was no other criminal evidence found on that machine. They also did not find any other information to show that the code bomb existed on that machine. Interestingly, the data from those two machines were destroyed when the first forensic company (recall the chain-of-custody issue mentioned earlier) was bought out by another company.

The testimony of Mr. Jones clarified that the data analyzed pointed to the user with the ID of "rduronio." The log data showed that this user was accessing the server from inside Duronio's home. Mr. Jones also clarified that the reason backup tapes were used instead of a bit-for-bit copy of the data was that the server data were damaged—so an image would not have been helpful. In addition, the IT workers at UBS were focusing on getting the system back online at the time of the attack, so the recovery efforts would

* Root user is a special user account on a UNIX system with the highest privilege level.
† A back door refers to an unauthorized way to access a computer system.
‡ Swap space is where inactive memory pages are held to free up physical memory for more active processes.

have written over data left on the server. Mr. Jones felt strongly that anything additional from a bit-for-bit copy would not contradict what was already discovered on the backup tapes anyway.

During the redirect* questioning, Mr. Faulkner was asked by the defense attorney, "Do you have a bottom line as to which username is responsible for the logic bomb?"

Mr. Faulker replied, "Root."

Since there were other system administrators with root access, the defense attorney asked a follow-up question, "Is there evidence which username, acting as root, was responsible?"

Mr. Faulker replied, "No."

Assistant US Attorney Mauro Wolf asked one additional question that turned it all around, "Bottom line…root did it. Roger Duronio could have acted as root?"

Mr. Faulker replied, "Yes."

#### *7.4.3.3 Other Strategies to Win the Case*

1. *Defense:* It was a conspiracy against Roger Duronio.
   a. The US Secret Service must have planted the evidence in Duronio's home. First, there was an unknown fingerprint on the hard copy of the code found in the house. Second, the Secret Service removed the computers from the house before the forensic image was taken of the machine. This may have been the reason they discovered the logic bomb code on the computers back in their office instead of in Duronio's home—because they put it there!
   b. The expert witness for the prosecution was biased and had an agenda because he was part owner of the company hired to do the forensic analysis.
   c. UBS was hiding evidence. The data from the workstations of the other two systems administrators were destroyed. The first forensics company was bought out and the evidence was destroyed in the process; this was not the doing of UBS. In addition, recall that the first forensics company hired hackers; therefore, the evidence they touched must be polluted.
   d. At one point, the defense also attempted to blame a scheduled penetration test of their system by Cisco.
2. *Prosecution:* Not much is needed here as they already had discovered enough data to convict Duronio. So, they pointed out that the background of the defense's forensic examiner was weak.

* Redirect questioning is the part of the trial process where the witness has an opportunity to refute information that may have damaged his or her testimony.

a. He had 2.5 years of forensics experience, most of which was gained during this case.
b. The defense's forensic examiner did not come to any conclusions following his forensic analysis.
c. The theories of the defense were all red herrings.* Why would all of those people (UBS, US Secret Service, Cisco, and the first forensics company) be after Roger Duronio?!

#### *7.4.3.4 Verdict*

Roger Duronio was found guilty. He was sentenced to 97 months without parole. He was also ordered to make $3.1 million in restitution to UBS Pain Webber.

### 7.4.4 After Action Report†

#### *7.4.4.1 What Worked Well for UBS-PW?*

1. **Resources:** The UBS IT executives had a plan and were able to get the system back up and running with the help of hundreds of consultants from IBM as well as hundreds of people from their own staff.
2. **Look for outside help:** They used a third party to lead the recovery effort (IBM) as well as a third party to do the investigation. Outsiders take an objective view of the problem. This is critical when an insider is suspected to be the cause of the problem.
3. **Find the problem and go nonstop:** The dedicated staff that worked nonstop on the problem was very effective in addressing the issue. They also did not stop until the problem was eradicated and the system was recovered.
4. **Backup:** The backup tapes restored the servers that were damaged.
5. **Learn from the experience:** UBS-PW did a postmortem on the event to learn from the experience.

#### *7.4.4.2 What to Do Differently Next Time*

1. **Remember that humans are the weakest link:** From weak passwords to disgruntled employees with access to critical systems—do not discount the damage that can be done.
2. **Enhance log reports:** The logs were good but could have been better. For example, they showed who switched to the root but not which commands the root ran on the system.

---

* Red herrings are issues that are distractions to the real issue.
† After three years of analyzing the UBS data, forensics expert Keith Jones came up with five points that helped UBS recover, as well as five points that will help them in the future.

3. **Limit root privileges:** Systems administrators should have root privileges only necessary to do their jobs. They do not need access to the whole system.
4. **Break the trust relationship:** Use better authentication between branch servers. In this situation, no authentication was required, so the logic bomb was easily pushed out to each server from the central server.
5. **Use encrypted protocols:** Use secure sockets layer (SSL) when allowing remote access to computers.

## References

Burson, S. 2010. Outsourcing information security. *CIO Magazine,* January 19.

Condon, R. 2007. How to mitigate the security risks of outsourcing. *ComputerWeekly.com*, December 5.

Kerth, N. n.d. An approach to postmorta, postparta, and post project reviews. http://c2.com/doc/ppm.pdf (retrieved February 12, 2013).

Ponemon Institute, LLC. March 2012. 2011 Cost of data breach study.

Schwartz, M. 2012. LinkedIn breach: Leading CISOs share 9 protection tips. *InformationWeekSecurity*, June 29.

*US v. Duronio.* Indictment USAO#2002R00528/JWD United States District Court, District of New Jersey.

## Bibliography

Gaudin, S. 2006. Defense witness in UBS trial says not enough evidence to make the case. *InformationWeek,* July 5.

———. 2006. Closing arguments to begin in trial of former UBS sys admin. *InformationWeek,* July 7.

———. 2006. At a glance: The UBS computer sabotage trial. *InformationWeek,* July 10.

———. 2006. Prosecutors: UBS sys admin believed "he had created the perfect crime." *InformationWeek,* July 10.

———. 2006. Defense: Government was out to get UBS sys admin. *InformationWeek,* July 12.

———. 2006. UBS trial aftermath: Top 10 tips for a successful postmortem. *InformationWeek,* July 21.

———. 2006. UBS trial aftermath: Five things UBS did right, and five things to improve on. *InformationWeek,* July 29.

INFORMATION TECHNOLOGY

**"Professor DeFranco has taken a very complex subject and distilled the knowledge into a very effective guide ... [and] has chosen a series of topics that connect to the real world of cyber security, incident response, and investigation. I think the book will make a valuable resource tool for anyone looking to get involved in the field, as well as those with years of experience."**

—**Robert L. Maley,** Founder, Strategic CISO

---

Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers in understanding the security risks involved in using or developing technology. Designed for the non-security professional, **What Every Engineer Should Know About Cyber Security and Digital Forensics** is an overview of the field of cyber security.

Exploring the cyber security topics that every engineer should understand, the book discusses:

- Network security
- Personal data security
- Cloud computing
- Mobile computing
- Preparing for an incident
- Incident response
- Evidence handling
- Internet usage
- Law and compliance
- Security and forensic certifications

Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the area of information security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding field.

CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K16045
ISBN-13: 978-1-4665-6452-7
90000
9 781466 564527