Chapter 1

The Need for Computer Forensics

Computer forensics is a fascinating field. As enterprises become more complex and exchange more information online, high-tech crimes are increasing at a rapid rate. The computer forensic industry has taken off in recent years, and it's no surprise that a profession once regarded as a vague counterpart of network security has grown into a science all its own. In addition, numerous companies and professionals now offer computer forensic services as a main line of business.

A computer forensic technician is a combination of a private eye and a computer scientist. Although the ideal background for this field includes legal, technical, and law enforcement experience, many industries as well as government and military organizations use professionals with investigative intelligence and technology proficiency. A computer forensic professional can fill a variety of roles such as private investigator, corporate compliance professional, or law enforcement official.

This chapter introduces you to the concept of computer forensics, while addressing computer forensic needs from two views—corporate policy and law enforcement. It will present some real-life examples of computer crime. It will help you assess your organization's needs and discuss various training methods used for practitioners and end users.

In this chapter, you'll learn more about:
- Defining computer forensics
- Understanding corporate forensic needs
- Understanding law enforcement forensic
- Training forensic practitioners
- Training end users
- Assessing your organization's needs

Defining Computer Forensics

computer forensics
Computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence.

The digital age has produced many new professions, but one of the most unusual is computer forensics. Computer forensics deals with the application of law to a science. The New Shorter Oxford English Dictionary defines *computer forensics* as "the application of forensic science techniques to computer-based material." In other words, forensic computing is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is acceptable in a legal proceeding. At times, it is more science than art; other times, it is more art than science.

Although it is similar to other forms of legal forensics, the computer forensics process requires a vast knowledge of computer hardware, software, and proper techniques to avoid compromising or destroying evidence. Computer forensic review involves the application of investigative and analytical techniques to acquire and protect potential legal evidence; therefore, a professional within this field needs to have a detailed understanding of the local, regional, national, and sometimes even international laws affecting the process of evidence collection and retention. This is especially true in cases involving attacks that may be waged from widely distributed systems located in many separate regions.

intrusion
Any unauthorized access to a computer, including the use, alteration, or disclosure of programs or data residing on the computer.

Computer forensics can also be described as the critical analysis of a computer hard disk drive after an *intrusion* or crime. This is mainly because specialized software tools and procedures are required to analyze, after the fact, the various areas where computer data is stored. Often this involves retrieving deleted data from hard drives and servers that have been subpoenaed to appear in court or seized by law enforcement.

electronic discovery or e-discovery
The process whereby electronic documents are collected, prepared, reviewed, and distributed in association with legal and government proceedings.

During the course of forensic work, you will run into a practice that is called *electronic discovery*, or *e-discovery*. Electronic discovery produces electronic documents for litigation. Data that is created or stored on a computer, computer network, or other storage media are included in e-discovery. Examples of such are e-mail, word-processing documents, plaintext files, database files, spreadsheets, digital art, photos, and presentations. Electronic discovery using computer forensic techniques requires in-depth computer knowledge and the ability to logically dissect a computer system or network to locate the desired evidence. It may also require expert witness testimony to explain to the court the exact method or methods by which the evidence was obtained.

Computer forensics has become a hot topic in computer security circles and in the legal community. It's a fascinating field with far more information available than can be analyzed in a single book, although this book will provide you with an understanding of the basic skills you'll need as a forensic investigator. Key skills in computer forensics are knowing the best places to look for evidence, and knowing when to stop looking. These skills come with time and experience.

In looking at the major concepts behind computer forensics, the main emphasis is on data recovery. To do that you must:

◆ Identify meaningful evidence

◆ Determine how to preserve the evidence

◆ Extract, process, and interpret the evidence

◆ Ensure that the evidence is acceptable in a court of law

All of these concepts are discussed in great detail throughout this book. Because computer-based information is fragile and can be easily fabricated, the simple presence of incriminating material is not always evidence of guilt. Electronic information is easy to create and store, yet computer forensics is a science that requires specialized training, experience, and equipment.

Real World Scenario

Tales from the Trenches: Why Computer Forensics Matters

A computer forensic examiner might be called upon to perform any of a number of different types of computer forensic investigations.

We have all heard of or read about the use of computer forensics by law enforcement agencies to help catch criminals. The criminal might be a thief who was found with evidence of his crime when his home or office computer was searched, or a state employee who was found to have stolen funds from public accounts by manipulating accounting software to hide funds transfers.

Most of us know that computer forensics is used every day in the corporate business world to help protect the assets and reputation of large companies. Forensic examiners are called upon to monitor the activities of employees, assist in locating evidence of industrial espionage, and provide support in defending allegations of misconduct by senior management.

Government agencies hire computer forensic specialists to help protect the data the agencies maintain. Sometimes, it's as simple as making sure IRS employees don't misuse the access they have been granted to view your tax information by periodically reviewing their activities. Many times, it's as serious as helping to defend the United States to protect the most vital top secret information by working within a counterintelligence group.

Every day, divorce attorneys ask examiners to assist in the review of personal computers belonging to spouses involved in divorce proceedings. The focus of such investigations usually is to find information about assets that the spouse may be hiding and to which the other spouse is entitled.

Continues

More recently, defense attorneys have asked forensic examiners to reexamine computers belonging to criminal defendants. Computer forensic experts have even been asked to reexamine evidence used in a capital murder case that resulted in the defendant's receiving a death sentence. Such reexaminations are conducted to refute the findings of the law enforcement investigations.

Although each of these areas seems entirely unique, the computer forensic examiner who learns the basics, obtains appropriate equipment, follows proper procedures, and continues to educate himself or herself will be able to handle each of these investigations and many other types not yet discussed. The need for proper computer forensic investigations is growing every day as new methods, technologies, and reasons for investigations are discovered.

Computer Crime in Real Life

An endless number of computer crime cases is available for you to read. Most of the crimes presented in the following sections come from the Department of Justice Web site, online at www.cybercrime.gov. In these cases, we'll look at several types of computer crime and how computer forensic techniques were used to capture criminals. The cases presented here illustrate some of the techniques that you will learn as you advance through this book. As a forensic investigator, you never know what you may come across when you begin an investigation. As the cases in this section show, sometimes you find more than you could have ever imagined.

Hacker Sentenced for Identity Thefts from Payment Processor and Retail Networks

Alberto Gonzalez, 28, led a hacking and identity theft ring that compromised record-breaking numbers of credit cards. For his part in the crimes, Gonzalez received the longest sentence imposed for criminal hacking to date. In March 2010, in separate cases, U.S. District Court judges sentenced Gonzalez to two 20-year prison terms for hacking into several retail networks and a major payment processor.

Gonzalez committed access device fraud, aggravated identity theft, computer fraud, conspiracy, and wire fraud. He and his associates hacked into major U.S. retailers, including the TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, and Sports Authority. He also led the group that breached the Dave and Buster's restaurant chain electronic payment systems. The second prison sentence, 20 years and one day, was for two counts of conspiracy for assisting others in breaching the networks of card processor Heartland Payment Systems,

supermarket chain, Hannaford Brothers Co. Inc., and nationwide convenience store chain, 7-Eleven.

Between July 2005 and his arrest in May 2008, Gonzalez and his group hacked into retail credit card payment systems by installing sniffer programs that captured payment card numbers used at the stores and by wardriving. Wardriving involves driving around in a car with a laptop computer looking for unsecured wireless computer networks. Gonzalez and his co-defendants stole more than 40 million credit and debit card numbers from major retailers. They sold the numbers and also committed ATM fraud by encoding the stolen data onto blank cards and then withdrawing cash from ATMs.

Gonzalez's ring hid and laundered their fraudulent gains by moving the money through bank accounts in Eastern Europe and using anonymous Internet-based currencies in the United States and abroad.

Gonzalez gave malware to other hackers that enabled them to bypass firewalls and anti-virus programs to break into companies' networks. (Malware is discussed in the Security Awareness section below.) Gonzalez admitted that his assistance allowed his co-conspirators to steal tens of millions of card numbers, adversely impacting hundreds of financial institutions.

In the largest investigation to date of its kind, the U.S. Secret Service worked abroad and in the United States using computer forensics to solve these cases. In July 2007, Secret Service in Turkey worked with Turkish agents to obtain Ukrainian suspect Maksym Yastremskiy's laptop while he danced at a nearby nightclub. After downloading data, U.S. agents returned the computer to Yastremskiy's hotel room. Instead of user names, Yastremskiy's accomplices used secure communication networks with numerical IDs.

Detectives noted Yastremskiy's chats with an American who sold millions of stolen credit card numbers to Yastremskiy. The American used the identity "201679996." The detectives worked with Carnegie Mellon University experts to link the numbers to a Russian e-mail address that belonged to Gonzalez. Ironically, Gonzalez had been working with the Secret Service as a consultant since 2003.

Shortly thereafter, the Secret Service arrested an Estonian hacker and found more than 40 million unsold credit card numbers linked to the break-ins at U.S. companies on two Latvian servers.

For months, Gonzalez hid in the National Hotel where he was living off more than $400,000 cash. He had buried another $1.1 million in the back yard of his parents' house. On May 7, 2008, agents raided Gonzalez's hotel room, condo, and parents' home. Gonzalez was then arrested.

Source: Wired.com, August 17, 2009, `http://www.wired.com/threat-level/2009/08/tjx-hacker-charged-with-heartland`; **U.S. Department of Justice, Office of Public Affairs**, `http://www.justice.gov/opa/pr/2010/March/10-crm-329.html`.

NOTE

Man Charged with Operating Online Scheme to Steal Income Tax Refunds

In June 2010, Mikalai Mardakhayeu was arrested and charged for his alleged role in an online phishing scam. The international scam was designed to steal U.S. taxpayer income tax refunds. Mardakhayeu is a Belarusian national living in Massachusetts. He was charged with conspiracy and wire fraud.

As alleged in the indictment, in 2006 and 2007, Mardakhayeu and his co-conspirators operated Web sites that offered lower-income taxpayers online tax return preparation and electronic tax return filing services at no cost. The fraudulent Web sites claimed to be authorized by the Internal Revenue Service (IRS). Co-conspirators in Belarus allegedly collected the data entered by taxpayers and then changed the returns so that the legitimate tax refund payments would be redirected to U.S. bank accounts that Mardakhayeu controlled. In some cases, his co-conspirators increased the amount of the claimed refund.

Allegedly, his co-conspirators electronically filed the modified returns with the IRS and various state treasury departments. As a result, the U.S. Treasury and state treasury departments deposited stolen refunds of approximately $200,000 into bank accounts that Mardakhayeu controlled. If convicted, he could be sentenced to 20 years in prison.

NOTE

Source: **U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS)**, http://www.justice.gov/criminal/cybercrime/marda-khayeuIndict.htm.

In this case, the forensic examiner might have found the files used to create the fraudulent Web sites. If the files were deleted, parts or all of them could have been recovered. Other evidence might include the actual data entered by the victims. The server logs and bank deposit records might have recorded who accessed the accounts. The forensic examiner has a wide variety of tools available to extract data and deleted information.

Newell Rubbermaid Network Hacked for Botnet and Adware Scams

In June 2008, a federal judge sentenced 21-year-old Robert Matthew Bentley to 41 months in prison and payment of $65,000 in restitution for conspiracy and computer fraud. Bentley and others (who are still being investigated) infected hundreds of computers in Europe with adware. The cost to detect and neutralize the adware was tens of thousands of dollars. Bentley and his co-conspirators

were paid for installing the adware through a Western European-based operation called "Dollar Revenue."

The investigation began when the U.S.-based Newell Rubbermaid Corporation and at least one other European-based company reported a computer intrusion against the companies' European networks to the London Metropolitan Police.

This complex, multiyear, international criminal investigation also involved the U.S. Secret Service, the Finland National Bureau of Investigation, London's Metropolitan Police Computer Crime Unit, and the Federal Bureau of Investigation (FBI). Each of these law enforcement organizations detected and responded to botnets of computers secretly controlled by Bentley and his co-conspirators. Evidence was found on computers in Florida that were used in the actual intrusions and to receive payment for placing the adware.

See U.S. Department of Justice, **Computer Crime and Intellectual Property Section (CCIPS)**, `http://www.justice.gov/criminal/cybercrime/bentleySent.pdf`. **See also "Hacker Pleads Guilty to Computer Fraud" at** `http://pcworld.about.com/od/adware/Hacker-Pleads-Guilty-to-Comput.htm`.

This case spanned several countries. National and international law enforcement agencies had to work together to track the illicit computer accesses. By installing the adware and accepting payments, the suspect unwittingly left a trail of forensic evidence. The evidence may have included items such as the parts of the program used to control the botnets.

Former Intel Employee Indicted for Alleged Heist of $1B in Trade Secrets

This case involves employee theft of valuable intellectual property. Stealing and selling proprietary information has become big business. When proprietary information is stolen, a computer forensic investigator may work in tandem with corporate human resources and compliance professionals to help examine not only how the theft occurred, but also provide evidence for prosecution. This case shows that the FBI takes a tough line against stealing data from former employers.

In 2008, Biswamohan Pani, 33, a former Intel employee, was indicted for wire fraud and the theft of more than $1 billion worth of trade secrets from Intel. The stolen information was valued in research and development costs and included mission-critical details about Intel's processes for designing its newest microprocessors. According to the affidavit, Pani told Intel management that he was resigning to work for a hedge fund and that he would use his accrued vacation until his termination date on June 11, 2008.

Pani remained on Intel's payroll through June 11, 2008, but he started work at Intel rival Advanced Micro Devices, Inc. (AMD) on June 2, 2008. From June 8 until June 11, 2008, Pani used his Intel laptop to access Intel's servers and download commercially sensitive data, including more than 100 sensitive documents, 13 of which were classified by Intel as "Top Secret." He also downloaded a document explaining how the encrypted Intel documents could be reviewed from an external hard drive after he left Intel. The indictment also alleged that Pani attempted to access Intel's computer network again two days after his last day at Intel. On July 1, 2008, proprietary Intel documents were located at Pani's home.

During his June 11 exit interview, Pani acknowledged his confidentiality obligations and falsely told Intel that he had returned all of Intel's property, including any documents or computer data.

Per the indictment, AMD personnel neither requested the stolen information nor knew that Pani had taken or would take it. Pani may have planned to use the information to further his career, with or without his employer's knowledge. Both Intel and AMD have assisted the FBI investigation.

If convicted, Pani faces up to 10 years on the trade secret charge, and an additional 20 years on each of the wire fraud counts.

NOTE

See U.S. Department of Justice, **Computer Crime and Intellectual Property Section (CCIPS)**, `http://www.justice.gov/usao/ma/Press%20Office%20 -%20Press%20Release%20Files/Nov2008/PaniBiswamohanIndictmentPR. html`. See also *Secure Computing Magazine*, **September 18, 2008,** `http://www. securecomputing.net.au/News/123155,amd-worker-charged-with-intel- theft.aspx`.

In this case, computer forensic evidence may include the date and time the files were downloaded as well as access information showing that Pani logged into the Intel servers. Time and date stamps are an important part of the computer forensic process. You will learn about these and other forensic techniques later in the book.

Figure 1.1 is from the Web site of the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice (`http://cybercrime.gov`). Here you can find a lot of useful information and additional cases.

The following examples illustrate that computer forensic investigators have no idea where their cases will end up. As a computer sleuth, you may be required to work across state lines and with various agencies. You may end up working with several companies in various countries. You may wind up at a dead end because it takes too long to get the information you need or the employer decides not to prosecute. The computer forensic world is full of surprises.

disaster recovery
The ability of an organization to recover from an occurrence inflicting widespread destruction and distress.

best practices
A set of recommended guidelines that outline a set of controls to improve internal and business processes, performance, quality and efficiency.

Figure 1.1   cybercrime.gov Web site *(U.S. Department of Justice)*
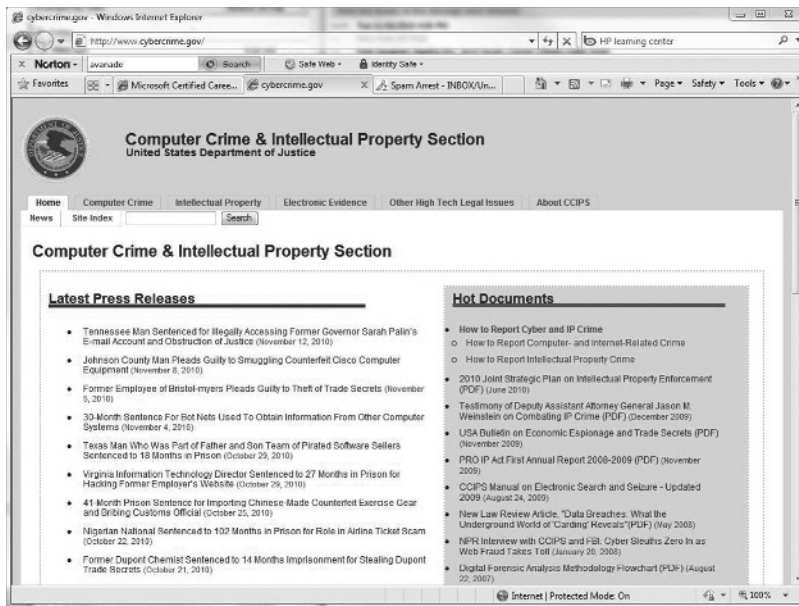
Corporate versus Law Enforcement Concerns

The needs of the corporate world and those of law enforcement differ on several levels. Law enforcement officials work under more restrictive rules than corporate agents or employees. If you assist law enforcement in an investigation, you may be considered "an agent of law enforcement" and you may be bound by the same restrictions that they encounter. When working with law enforcement, it's important to be aware of these ramifications, especially if you're working without a court order. This scenario could also open you up to civil litigation when complying with such requests, so it's always advisable to seek legal counsel. In the corporate world, all that is generally required to begin an investigation—to access servers, network systems, routers, and so forth—is the written approval of the corporate agent with the appropriate level of authority for such activities. On the other hand, law enforcement is subject to multiple laws regarding not only how but under what circumstances evidence can be seized. Often, forensic investigators working in law enforcement need a court order before they may examine computer systems, networks, routers, and so on. Face it: There is a big difference between a company deciding to log router traffic and a local or federal law enforcement officer asking the company to log the traffic.

incident
A threatening computer security breach that can be recovered from in a relatively short period of time.

incident response
The action taken to respond to a situation that can be recovered from relatively quickly.

Both law enforcement and corporate practitioners follow a set of *best practices* set forth by various agencies. For law enforcement, a set of best practices exists for electronic discovery and proper retrieval of data. The corporate world also established best practices for security and best practices for determining what comprises an *incident*. These best practices inform *incident response* procedures, which describe how to react to an incident. Because disasters are usually of a larger magnitude, best practices for disaster recovery may affect both electronic discovery and retrieval of data. The focus of this book is to provide information that can be used in either discipline—corporate computer forensics or law enforcement computer forensics—and is not specifically aimed at law enforcement.

Corporate Concerns: Detection and Prevention

intrusion detection
Using software and hardware agents to monitor network traffic for patterns that may indicate an attempt at intrusion.

Every day new articles are written about network security and vulnerabilities in software and hardware. This visibility has caused security to become a priority in most companies. Corporate efforts to make sure a network is secure generally are focused on how to implement hardware and software solutions, such as *intrusion detection*, web filtering, spam elimination, and patch installation. The SQL Slammer *worm* infected 200,000 computers running Microsoft's SQL Server. Ninety percent of all vulnerable servers were infected in the first 10 minutes after the worm was released on the Internet. Dealing with the threat of network damage through an intrusion or *virus* is a part of everyday life for corporate IT professionals, whereas forensic experts focus on the examination, analysis, and evaluation of computer data to provide relevant and valid information to the courts.

security policies
Specifications for a secure environment, including such items as physical security requirements, network security planning details, a detailed list of approved software, and human resources policies on employee hiring and dismissal.

Corporate focus is on minimizing the potential damage that may result from unauthorized access attempts through the prevention, detection, and identification of an unauthorized intrusion. This is done mainly by putting *security policies* in place that dictate the level of security for various areas and computers. Along with these policies, incident response and disaster recovery plans set forth procedures for investigations, including when, who, and how to contact law enforcement.

Companies can access Web sites to find out about new vulnerabilities or security best practices. It is in the best interest of any company to assign someone to check this information on a regular basis to ensure that the network is protected.

virus
A program or piece of code that is loaded onto a computer without the user's knowledge and is designed to attach itself to other code and replicate. The virus replicates when an infected file is executed or launched.

You'll find in many corporate environments that incidents are not reported, often due to the issue of legal liability. The "Let's just quietly fix it" approach to security incidents is common in the corporate world. Some laws now hold senior management responsible for data breaches. A company is potentially liable for damages caused by a hacker's using one of its computers, and a company might have to prove to a court that it took reasonable measures to defend itself from hackers.

The following federal laws address security and privacy and affect nearly every organization in the United States.

> The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted on August 21, 1996, to ensure the portability, privacy, and security of medical information. HIPAA dictates that only patients, agents they designate, and their health-care providers have access to the patients' medical information. HIPAA requires that Patient Health Information (PHI) be kept private and secure. It imposes stiff fines and jail time both for health-care institutions and individuals who disclose confidential health information to unauthorized parties.

> The Gramm-Leach-Bliley (GLB) Act requires financial institutions to ensure the security and confidentiality of the personal information that they collect. This includes information such as names, addresses, phone numbers, income, and Social Security numbers. Basically, financial institutions are required to secure customer records and information regardless of size of the information files. Among other institutions, GLB covers check-cashing businesses, mortgage brokers, real estate appraisers, professional tax preparers, courier services, and retailers that issue credit cards to consumers.

> The Sarbanes-Oxley Act, named for the two Congressmen who sponsored it, was passed to restore the public's confidence in corporate governance by requiring chief executives of publicly traded companies to personally validate financial statements and other information. Congress passed the law to prevent future accounting scandals such as those committed by Enron and WorldCom. Under the law, executives who sign off on internal controls can face criminal penalties if a breach is detected. In other words, if someone can easily get into a secure or private part of your system because you use a three-character password such as "dog," you will be noncompliant with Sarbanes-Oxley.

Compliance is becoming more important to businesses, which face an increasing number of laws and regulations that involve e-discovery obligations and data breach notification laws. For example, a new Massachusetts law protects residents' personal data from breaches and sets a fine of $5,000 for each record lost. This means a company could be fined $1 million for losing a laptop computer containing personal data on 200 Massachusetts residents.

The new law applies to businesses in Massachusetts and to any company that keeps personal data on the state's residents. The law requires companies to act to prevent breaches, not just to notify victims after a breach has occurred. Businesses must encrypt data in motion and at rest, including information on portable devices such as USB drives, laptop computers, and smartphones.

worm
Similar in function and behavior to a virus, except that worms do not need user intervention. A worm takes advantage of a security hole in an existing application or operating system and then finds other systems running the same software and automatically replicates itself to the new hosts.

Often, a company that is the victim of a security breach does not know which law enforcement entity to call. Company management might feel that the local or state police will not be able to understand the crime and that the FBI and Secret Service are not needed. In addition, management might be afraid that the intrusion will become public knowledge, harming investor confidence and chasing away current and potential customers. They might also fear the effect of having critical data and computers seized by law enforcement.

An investigation can seriously jeopardize the normal operations of a company, not only for the customers but for employees as well. A disruption in the workplace causes confusion and upsets employee schedules. Furthermore, cases are often hard to pursue if a suspect is a juvenile or an intruder is from another country. In many states, the damages inflicted by an intruder are too small to justify prosecution. Last, pursuing such matters takes a long time and can be costly.

NOTE   **Many businesses perceive that there is little benefit to reporting network intrusions.**

Law Enforcement Concerns: Prosecution

Whereas the corporate world focuses on prevention and detection, the law enforcement realm focuses on investigation and prosecution. Each state has its own set of laws that govern how cases should be prosecuted. For cases to be prosecuted, evidence must be properly collected, processed, and preserved. In later chapters, we'll go through these procedures. Technology has dramatically increased the universe of discoverable electronic material, thereby making the job of law enforcement much more complex. Electronic evidence can include any and all electronically stored information that is in digital, optical, or analog form. Not only does evidence include electronic data, it also includes electronic devices such as computers, CD-ROMs, floppy disks, cellular telephones, pagers, and digital cameras.

Real World Scenario

22-Year Old Tennessee Man Convicted for Hacking into Sarah Palin's E-mail Account

On April 30, 2010, a federal jury in Tennessee convicted David C. Kernell, now 22, of intentionally obtaining unauthorized access to Sarah Palin's e-mail account. Kernell, the son of a Tennessee state Representative, was also convicted of obstruction of justice. Kernell was found not guilty of wire fraud. The judge declared a mistrial on the identity theft charge because the jury was unable to reach a verdict on that charge. Kernell turned himself into federal authorities.

Continues

Evidence presented at trial showed that on Sept. 16, 2008, Kernell accessed Palin's personal e-mail account. He reset her account password by providing Palin's birth date and zip code to Yahoo's password retrieval system. According to the evidence, Kernell read the contents and captured screenshots of the e-mail directory, e-mail content, and other personal information. Kernell posted screenshots of Palin's personal information and e-mail messages to a public Web site. Kernell also changed her password to a new one and posted the new password, allowing the account to be accessed by others.

Evidence also showed that after he became aware of a possible investigation by the FBI, Kernell deleted electronic evidence to obstruct the imminent FBI investigation. As of the writing of this book, Kernell's sentencing is scheduled for late October 2010. Kernell faces a maximum of one year in prison and a $100,000 fine for unauthorized access as well as 20 years in prison and a $250,000 fine for obstruction of justice.

Source: U.S. Department of Justice, Federal Bureau of Investigation, Knoxville,
`http://knoxville.fbi.gov/dojpressrel/pressrel10/kx043010.htm`

For a case to stand up in court, most evidence must be attested to by a witness. In the case of electronic evidence, who is the witness of a computer making a log entry? How can a law enforcement officer show that the other 15 accounts logged in at the time didn't commit the deed? Despite the relative infancy of the law, electronic data is finding its way into the courtroom and is profoundly impacting many cases.

Courts are generally not persuaded by challenges to the authenticity, best evidence rule, chain of custody, and so on of electronic data introduced at trial. This type of issue has been brought up in court several times. A good example is *United States v. Tank*. The court addressed the question of the authentication of Internet chat room logs that were maintained by one of the co-defendants. The defendant claimed that the government did not have a sufficient foundation for the admission of the logs. The government provided evidence linking the screen name used by the defendant to the defendant. The government evidence also included testimony from one of the co-defendants about the method he used to create the logs and his recollection that the logs appeared to be an accurate representation of the conversations among the members. The court ruled in favor of the government, declaring that the government made a satisfactory showing of the relevance and authenticity of chat room log printouts.

With the increase of cybercrime, keeping up with caseloads has become nearly impossible. Department of Public Safety (DPS) crime lab personnel barely have time to answer the phone. How does law enforcement determine the priority of the complaints that they investigate and prosecute? Generally speaking, the following factors help determine which cases get priority:

The Amount of Harm Inflicted Crimes against children or violent crimes usually get high priority, along with crimes that result in large monetary loss.

Crime Jurisdiction   Crimes that affect the local populace are usually chosen, especially when resources are taken into consideration.

Success of Investigation   The difficulty of investigation and success of the outcome weigh heavily in determining which cases are investigated.

Availability and Training of Personnel   Often crime investigations that don't require a large amount of manpower or very specific training take precedence.

Frequency   Isolated instances take a lower priority than those that occur with regular frequency.

In addition, some associations offer help and guidance not only to law enforcement but the corporate world as well. The High Technology Crime Investigation Association (HTCIA) is one such organization. The national Web site, `http://htcia.org`, links to chapters throughout the world, which include information on local laws associated with computer crimes.

Training

To fight cybercrime effectively, everyone who deals with it must be educated. This includes the criminal justice and the IT communities, as well as everyday users. Imagine what would happen to evidence if a law enforcement officer wasn't properly trained and, as a result of his or her actions, a good portion of evidence was destroyed. Many times, the judge or jury does not understand the topics discussed or lacks the technical expertise to interpret the law. What would happen in a complex case if the jury, prosecutor, and judge did not understand computer-related evidence? More likely than not, the defendant would end up getting away with the crime.

We are faced with many scenarios where this is true, but probably none more vexing than cases involving child pornography. Child pornography issues present circumstances in which the prosecution might have to prove that a photograph is one of a real child owing to rulings on virtual pornography. Pornographic pictures and videos with images that look like children need to be evaluated to determine if the subject is a minor and whether or not the subject is real or virtual. A defendant may claim that the images are of adults or virtual children. Experts may render opinions based on experience and training. Forensic investigators may use techniques such as skin tone analysis or verification against a database of items already recognized as real. The National Center for Missing and Exploited Children (NCMEC) (`http://www.missingkids.com/missingkids/servlet/PublicHome Servlet?LanguageCountry=en_US`) maintains a database of real images against which law enforcement personnel can compare alleged child pornographic images for verification. A complete analysis may also include more standard forensic tasks, such as generating file listings, extracting web browser histories, processing email

and text messages, manually reviewing pictures and videos, and extracting metadata. However, not all cases go to court, and the role of a forensic investigator can vary.

Before deciding what type of specific training you need, evaluate the role you want to fill so you get the most benefit. Here are common roles that can involve computer forensics:

◆ Law enforcement officials

◆ Legal professionals

◆ Corporate human resources professionals

◆ Compliance professionals

◆ Security consultants providing incident response services

◆ System administrators performing incident response

◆ Private investigators

The next sections discuss the types of computer forensic employees in both the corporate and law enforcement worlds and the types of training available for them.

Forensic Practitioners

The following types of people and organizations sometimes hire computer forensic specialists:

◆ Civil litigators can utilize personal and business computer records in cases involving fraud, divorce, and harassment.

◆ Insurance companies can sometimes reduce costs by using computer evidence of possible fraud in accident, arson, and workman's compensation cases.

◆ Corporations hire computer forensic specialists to obtain evidence of embezzlement, theft, and misappropriation of trade secrets.

◆ Individuals sometimes hire computer forensic specialists to support claims of wrongful termination, sexual harassment, and age discrimination.

◆ Law enforcement officials sometimes require assistance in pre-search warrant preparation and post-seizure handling of computer equipment.

◆ Prosecutors and defense attorneys in criminal and civil proceedings often use evidence uncovered by computer forensic specialists.

◆ Criminal prosecutors use computer evidence in cases such as financial fraud, drug and embezzlement record-keeping, and child pornography.

All of these industries rely on properly trained computer forensic investigators. The following sections describe some of the training available to both corporate and

law enforcement worlds. The role that you play as a computer forensic investigator will ultimately decide which type of training is right for you.

Law Enforcement

The position an individual holds in the criminal justice community dictates the type of training required. Here are some examples of the types of training needed in several professions:

- ◆ Legislators need to understand the laws that are proposed and that they are passing.
- ◆ Prosecuting attorneys should have training on electronic discovery and digital data, and how to properly present computer evidence in a court of law.
- ◆ Detectives should have hands-on training in working with data discovery of all types and on various operating systems.

When law enforcement professionals are originally trained at the academy, they should receive some type of basic training on computer crime and how to investigate such crimes. Ideally, all criminal justice professionals would receive training in computer crimes, investigations, computer network technologies, and forensic investigations. Here are some ways to get the training needed to pursue a career in computer forensics:

- ◆ Key Computer Service Certified Computer Examiner (CCE) BootCamp: `http://www.cce-bootcamp.com/`
- ◆ The SANS Institute's computer security training courses: `www.sans.org`
- ◆ The International Association of Computer Investigative Specialists (IACIS) forensic examiner courses: `http://www.iacis.com`

Many local community colleges and universities offer classes in computer forensics. Law enforcement professionals can take advantage of them without having to pay the high cost of classes offered by private firms. An excellent resource for law enforcement is the International Association for Computer Investigative Specialists (IACIS), online at `http://www.iacis.com/`.

Corporate

Frequently, security and disaster recovery projects aren't funded because they don't produce revenue. An Ernst & Young annual security survey of 1,400 organizations states that only 13 percent think that spending money on IT training is a priority. This shows that training is needed not only for IT professionals but for management as well.

In the corporate world, just as in the criminal justice world, the position an individual holds in an organization dictates the type of training they need. For end

users to buy into security, management must buy in first. Managers have a legal responsibility to police what is happening within their own computer systems, as demonstrated by the Sarbanes-Oxley Act. Management training is usually geared more toward compliance issues and the cost of putting preventative measures in place. IT professionals, on the other hand, need training geared more toward return on investment (ROI) in order to obtain funding for security projects and computer crime awareness, which includes new vulnerabilities. They should also be trained on applicable laws and regulations, how crimes are investigated, and how crimes are prosecuted. This training can help eliminate the reluctance that organizations have about contacting law enforcement when security breaches occur or when crimes are committed.

Education for every level of practitioner can be found on the SANS (SysAdmin, Audit, Network, Security) Web site at `http://www.sans.org/security-resources.php` (Figure 1.2). The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs are designed to educate security professionals, auditors, system administrators, network administrators, chief information security officers, and chief information officers.

Figure 1.2   SANS Security Resources Web site

End Users

Legislation such as Sarbanes-Oxley will not change behaviors simply because it is the law. This is like speeding. Laws against driving over the speed limit do not stop some people from speeding: Many speeders are repeat offenders. Why? It's because certain behaviors are difficult to change. A person's behavior is based on their principles and values. People adopt new patterns of behavior only when their old ones are no longer effective.

The goal of training is to change behavior. An effective training program helps the workforce adopt an organization's principles and values. As already mentioned, management must be trained, buy in, and become an integral part of user education and the training process for everyone to take such training seriously. Only then will users adopt more secure behaviors.

The hardest environment to control is the end user's environment. Training and education are vital to any organization with computer users and Internet access.

Security Awareness

malware
Another name for malicious code. This includes viruses, logic bombs (slag code or a delayed-action virus), and worms.

social engineering
A method of obtaining sensitive information about a company through exploitation of human nature.

A network is only as strong as its weakest link. We hear this phrase time and time again. Humans are considered to be the weakest link. No matter how secure the hardware and software are, if users aren't taught the dangers of social engineering, e-mail scams, and *malware,* the network can be jeopardized with a phone call or simple mouse click.

Social engineering plays on human nature to carry out an attack. Which is easier, getting an employee to give you a password or running password-cracking software? Obviously, getting an employee to give you a password eliminates a lot of effort on the part of a criminal. Social engineering is hard to detect because employers have very little influence over lack of common sense or ignorance on the part of employees. That said, employee education is the best counter against ignorance. Most business environments are fast-paced and service-oriented. Human nature is trusting and often naïve.

Take this scenario as an example. A vice president calls the help desk and states that he's in big trouble. He's trying to present a slideshow to an important client and has forgotten his password; therefore, he can't log onto the company Web site to make the presentation. He changed his password yesterday and can't remember the new one. He needs it right away because he has a room full of people waiting, and he's starting to look incompetent. The client is extremely important and could bring millions of dollars in revenue to the company. However, if the help desk staff member supplies the password as requested, without verifying that the caller is who he says he is, the help desk staff member could be giving access to an intruder.

If you think that this is an unlikely scenario, consider that in July 2010, a contest at the annual Defcon convention pitted social engineers against Fortune 500 companies. Participants in the contest had no problem getting data from Fortune 500 companies. Data that the contestants collected from employees included the operating system and service pack number they use, the e-mail client and antivirus software they use, and the name of their local wireless network.

Network World reported on this contest on July 30, 2010 (`http://www.net-workworld.com/news/2010/073110-how-to-steal-corporate-secrets.html`). The first contestant, Wayne, was an Australian security consultant given the task to call a major U.S. company and get any data that could be used in a computer attack. From inside a soundproof booth in front of the audience, Wayne contacted an IT call center and talked with an employee. Wayne claimed to be a consultant from KPMG, an international firm that provides audit, tax, and advisory services, who was performing an audit and faced pressure from an approaching deadline. The call center employee was new and had only been with this employer for a month.

Ignoring the call center employee's request for his employee number, Wayne immediately launched into a routine about his boss being on his back, and how he really needed to wrap up this audit. Within a few minutes, the new worker appeared willing to give out whatever information Wayne requested. The call center employee even visited a fake web page for KPMG to which Wayne directed him. At the end of the call, Wayne asked the employee what beer he preferred and promised to buy him one.

When creating a security-awareness program, organizations should keep these goals in mind:

◆ Evaluate compelling issues.

◆ Know laws and policies for protecting data.

◆ Look at values and organizational culture.

◆ Set baseline knowledge requirements.

◆ Define best practices.

◆ Make lasting cultural and behavioral changes.

◆ Create positive approaches and methods.

For each topic in the awareness program, the two most important ideas to convey to end users and IT employees are what a potential incident looks like, and what the end user should do about it. If you need help putting together these policies, the National Institute of Standards and Technology (NIST) has some great information in its Computer Security Resource Center (CSRC) at `http://csrc.nist.gov/groups/SMA/ate/` (Figure 1.3).

Figure 1.3   NIST Computer Security Resource Center Web site
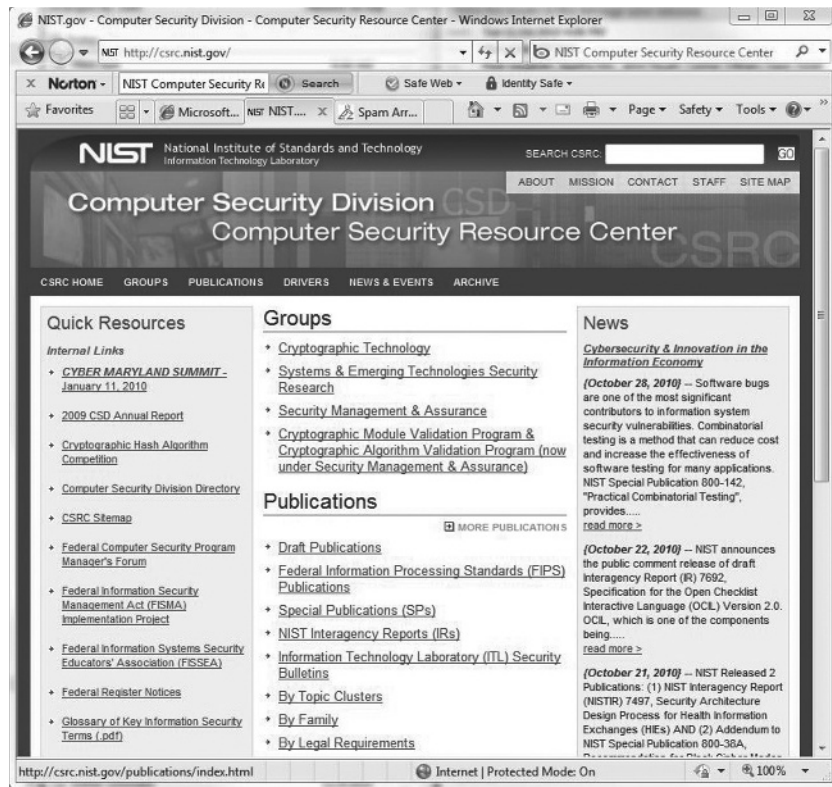
All organizations that rely on computer technology or use sensitive data should have a security awareness and training program. Such a program is required by various laws for specific industries, such as the Sarbanes-Oxley Act for all publically held companies, the Gram-Leach Bliley Act for financial institutions, and the Health Insurance Portability and Accountability Act for health-care entities. If you need more information on these federal security and privacy laws, see the "Corporate Concerns: Detection and Prevention" section earlier in this chapter. Many individual states also have laws that require businesses to protect sensitive personal and financial data, and to report data breaches. An effective awareness and training program can reduce an organization's risk profile, allow earlier identification of an attack or breach, and may even prevent loss of important forensic data when an attack occurs.

What Are Your Organization's Needs?

Each organization is different. As a professional, it is your job to assess your organization's specific needs.

Law enforcement professionals may determine that their caseloads are too extensive for the manpower they have. Maybe the equipment they are using is outdated. Perhaps they have issues with a particular type of software.

Corporate organizations may want to make sure they formulate security policies by assessing risk, threats, and their exposure to determine how best to keep their networking environment safe. Corporations can also have outdated equipment or applications, making their networks more vulnerable.

Because every organization is different, with different policies and requirements, there are no "one size fits all" rules that cover all the security bases. Training and education make a good start, but you must constantly update your knowledge of hardware, software, and threats. You should recognize how they affect your work and your organization so that you can continuously reassess your vulnerabilities. Remember, a computer forensic technician is a combination of a private eye and a computer scientist.

Security experts are able to monitor vast amounts of data. They can track Internet access, read employee e-mails, record phone calls, and monitor network access. How much you monitor depends on how much information you want to store. Remember that your monitoring plan should be clear-cut and built around specific goals and policies. Without proper planning and policies, you can quickly fill your log files and hard drives with useless or unused information. Here are some items to consider as you get ready to implement a monitoring policy:

◆ Identify potential resources at risk within your environment (for example, sensitive files, financial applications, and personnel files).

◆ After resources are identified, set up the policy. If a policy requires auditing large amounts of data, be sure the hardware has the necessary storage space, as well as sufficient processing power and memory.

◆ Make time to review the logs. The information in log files won't help protect against a system compromise if you don't read it for six months.

You can monitor as much or as little as you want, but if you don't read the logs, they cannot serve their intended purpose.

NOTE

Monitoring can be as simple or complex as you want to make it. Be consistent regardless of the plan you create. Many organizations monitor an extensive amount of information, while others, especially small ones, may monitor little or nothing. Just remember that it will be quite difficult to catch an intruder if you don't monitor anything.

Terms to Know

best practices

computer forensics

disaster recovery

electronic discovery

incident

incident response

intrusion

intrusion detection

malware

security policies

social engineering

virus

worm

Review Questions

1. What is electronic discovery?

2. Name some examples of electronic discovery items.

3. The recovery of data focuses on what four factors?

4. Who works under more restrictive rules, law enforcement officials or corporate employees?

5. What is incident response?

6. Why is social engineering hard to prevent and detect?

7. Why aren't incidents reported in many corporate environments?

8. What law was passed to avoid future accounting scandals such as those involving Enron and WorldCom?

9. Name some factors that help to determine which criminal cases get priority.

10. Name a good resource for computer forensic training for law enforcement.