4375.book Page 1 Monday, October 18, 2004 3:13 PM

Chapter 1

The Need for Computer Forensics

In This Chapter

- Defining computer forensics
- Understanding corporate forensic needs
- Understanding law enforcement forensics needs
- Training practitioners
- Training end users
- Assessing your organization's needs

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 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. 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, a myriad of industries 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 both sides—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.

COPYRIGHTED MATERIAL

4375.book Page 2 Monday, October 18, 2004 3:13 PM

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 and software in order to avoid the accidental invalidation or destruction of evidence and to preserve the evidence for later analysis. 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.

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

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 the various areas where computer data is stored, after the fact. Often this involves retrieving deleted data from hard drives and servers that have been subpoenaed in court or seized by law enforcement. During the course of forensic work, you will run into a practice that is called *electronic discovery*. Electronic discovery produces electronic documents for litigation. Items included in electronic discovery include data that is created or stored on a computer, computer network, or other storage media. Examples of such are e-mail, word-processing documents, plaintext files, database files, spreadsheets, digital art or photos, and presentations. Electronic discovery using computer forensics 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 popular topic in computer security circles and in the legal community. Even though it is a fascinating field, due to the nature of computers, far more information is available than there is time to analyze, and a key skill is to know when to stop looking. This is a skill that comes with time and experience. For now, let's look at the major concepts behind computer forensics. The main emphasis is on recovery of data. To do that you must:

- Identify the evidence
- Determine how to preserve the evidence

4375.book Page 3 Monday, October 18, 2004 3:13 PM

- 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 planted, rarely is the simple presence of incriminating material the evidence of guilt. So as you can see, 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 Is Important

A computer forensics examiner might be called upon to perform any of a number of different types of computer forensics 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. Forensics 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 forensics 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 by protecting the most vital top secret information by working within a counter intelligence group.

Every day, divorce attorneys ask examiners to assist in the examination 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

4375.book Page 4 Monday, October 18, 2004 3:13 PM

More recently, defense attorneys have asked forensic examiners to reexamine computers belonging to criminal defendants. Computer forensics experts have even been asked to reexamine evidence used in a capital murder case that resulted in the defendant 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 forensics 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 forensics investigations is growing every day as new methods, technologies, and reasons for investigations are discovered.

Real-Life Examples of Computer Crime

An endless number of computer crime cases are available for you to read. Most of the ones in the following sections come from the Department of Justice website, which is at `http://www.cybercrime.gov`. In these cases, we'll look at several types of computer crime and how computer forensic techniques were used to capture the criminal. The five cases presented here illustrate some of the techniques that you will become familiar with 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 Pleads Guilty to Illegally Accessing New York Times Computer Network

Adrian Lamo, 22, was charged in a Manhattan federal court with hacking into the internal computer network of the New York Times. Lamo illegally accessed a database containing confidential information such as home telephone numbers and Social Security numbers for over 3,000 contributors. The records he accessed included entries for former President Jimmy Carter, Democratic campaigner James Carville, former secretary of state James Baker, actor Robert Redford, columnist William F. Buckley, Jr., and radio personality Rush Limbaugh among others.

Investigators found that the hacker had added an entry for Adrian Lamo, listing personal information such as a cellular telephone number, (415) 505-HACK, and a description of Lamo's areas of expertise including computer hacking, national security, and communications intelligence. Lamo also created five fictitious user accounts with a fee-based, online subscription service that provides news and legal and other information to customers. Over the course of three months, those five accounts were used to conduct upwards of 3,000 searches, incurring charges of approximately $300,000.

4375.book Page 5 Monday, October 18, 2004 3:13 PM

NOTE

Source: Security Focus, September 5, 2003, `http://www.securityfocus.com/news/6888`**; U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS),** `http://www.cybercrime.gov/lamoPlea.htm`.

In addition, Lamo admitted responsibility for a series of other computer intrusions on networks at Cingular, Excite@Home, MCI WorldCom, Microsoft, SBC Ameritech, and Yahoo!. If convicted, Lamo faces a maximum sentence of 15 years in prison and a $500,000 fine.

By using computer forensic techniques, his trail could be traced through proxy server logs, the accounts he created while on the internal network, and unauthorized LexisNexis searches for such information as his name, other individuals with the last name "Lamo," searches using his parents' Northern California home address, and searches for some of his known associates.

Stealing and selling proprietary information has become big business. The next two cases are examples of just that. When proprietary information is stolen, a computer forensic investigator may work in tandem with corporate human resources and compliance professionals to help not only examine how the theft occurred but also provide evidence for prosecution.

Man Pleads Guilty to Hacking Intrusion and Theft of Data Costing Company $5.8 Million

Daniel Jeremy Baas, age 25, of Milford, Ohio, pled guilty to exceeding authorized access to a protected computer and obtaining information. Baas was charged with illegally accessing a protected computer and stealing customer databases from Acxiom, a Little Rock, Arkansas-based company that maintains customer information for automotive manufacturers, banks, credit card issuers, and retailers, among others. The intrusion and theft of data cost Acxiom more than $5.8 million, which, in addition to the value of the stolen information, included employee time and travel expenses, and the cost of security audits and encryption software.

Baas worked as a computer systems administrator for a Cincinnati-based company that did business with Acxiom, which made files available for download for Baas' employer. With that access, Baas ran a password-cracking program on Acxiom computers, illegally obtaining about 300 passwords, including one with administrator-level privileges. That user account allowed him to download files belonging to other Acxiom customers, which contained confidential identification information.

Baas faced a maximum prison sentence of five years, a fine of $250,000 or twice the amount of gain or loss, and three years of supervised release.

NOTE

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.cybercrime.gov/baasPlea.htm`.

4375.book Page 6 Monday, October 18, 2004 3:13 PM

In this case, the forensic examiner might have found the program used to crack the password. If the program was deleted, parts of all of it could have been recovered as well as the password file. Other evidence might include the actual downloaded files or fragments of them. The download program itself might have a log file that would have recorded who accessed the program and what was downloaded. The forensic examiner has a wide variety of tools available to extract data and deleted information.

Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information

Brian A. Salcedo, Adam W. Botbyl, and Paul G. Timmins were indicted on November 19, 2003, by a federal grand jury on sixteen counts of unauthorized computer access, attempted possession of unauthorized access devices computer fraud, conspiracy, intentional transmission of computer code, and wire fraud.

Salcedo, Botbyl, and Timmins first accessed the wireless network at a Lowe's retail store in Southfield, Michigan. They subsequently hacked into the central computer network at Lowe's Companies, Inc. in North Carolina and then into computer systems in Lowe's retail stores across the United States. The men installed a program on computers in several of the retail locations that captured customers' credit card account numbers. If convicted on all counts, Salcedo, Botbyl, and Timmins face maximum sentences of 170 years in prison.

NOTE

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.cybercrime.gov/salcedoIndict.htm`.

The previous case spanned several states. Several federal agencies and various state and local agencies had to work together to track the illicit computer accesses. By compromising the system and then capturing credit card information, the three suspects unwittingly left a trail of forensic evidence. Some of the evidence possibly included the actual credit card information or remnants of this information, in addition to the program or parts of the program used to capture the information and log file records that indicated access to various locations on the corporate network.

The next case is one of employee revenge and destruction. This type of criminal activity has become common as more employees who are computer savvy try to find ways to get back at employers.

4375.book Page 7 Monday, October 18, 2004 3:13 PM

Former Chief Computer Network Program Designer Arraigned for Alleged $10 Million Computer Software Bomb

Timothy Allen Lloyd, of Wilmington, Delaware, was sentenced to 41 months in prison for launching a programming bomb on Omega Engineering Corp.'s network that resulted in approximately $10 million in damages. Lloyd, a computer network program designer for New Jersey-based Omega for 11 years, was terminated from his position on July 10, 1996. Twenty days later, a *logic bomb* was activated that permanently deleted all of the company's design and production software for measurement and control instruments used by the U.S. Navy and NASA.

logic bomb
A virus or other program that is created to execute when a certain event occurs or a period of time passes. For example, a programmer might create a logic bomb to delete all his code from the server on a future date, most likely after he has left the company.

In addition to the monetary loss in sales and contracts, the attack led to 80 layoffs within Omega. The case is apparently one of the most expensive computer sabotage cases in U.S. Secret Service history.

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.cybercrime.gov/lloydSent.htm`.

NOTE

In this case, computer forensic evidence may include the actual program or logic bomb, the date and time the file was created, and the username of the file creator. 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.

The following graphic is from the website of the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice. Here you can find a lot of useful information and additional cases. The last case concerns a computer crime committed by a child.

4375.book Page 8 Monday, October 18, 2004 3:13 PM

Juvenile Computer Hacker Sentenced to Six Months in Detention Facility

A juvenile, who goes by the name "c0mrade" on the Internet, accepted responsibility in a U.S. District Court in Miami for illegally accessing a military computer used by the Defense Threat Reduction Agency (DTRA), stealing usernames and passwords, and capturing e-mail messages exchanged between DTRA staff. DTRA, a Department of Defense agency, is responsible for reducing the threat from nuclear, biological, chemical, conventional, and special weapons to the United States and its allies.

backdoor
A software program that allows access to a system without using security checks.

Over a two-month period beginning in August 1999, the juvenile accessed the DTRA network by secretly installing a *backdoor* on a server in Virginia. In addition to capturing over 3,300 e-mail messages, he acquired at least 19 usernames and passwords of DTRA staff, 10 of which were on military computers.

The juvenile also admitted to illegally accessing 13 computers located at NASA's Marshall Space Flight Center on June 29 and 30, 1999, and downloading proprietary software worth approximately $1.7 million. The intrusions and data theft forced NASA to shut down the computer systems for 21 days in July, resulting in approximately $41,000 in contractor labor and computer equipment replacement costs.

NOTE

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.cybercrime.gov/comrade.htm`.

This case marks the first time a juvenile hacker was sentenced to serve time. In addition to his six-month sentence in a detention facility, c0mrade was required to write letters of apology to the Department of Defense and NASA and allowed public disclosure of information about the case.

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

What kind of information was found that led to his arrest and conviction? A forensic investigator might have been able to recover a significant number of the captured e-mails if they were deleted. They might have been hidden in a directory or on a hard disk partition. In addition, a forensic investigator probably was able to trace the downloaded software, possibly to the suspect's computer.

best practices
A set of recommended guidelines that outline a set of good controls.

These cases 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 up at a dead end because it takes too long to get the information you need or the employer decides not to prosecute. At any rate, the computer forensics world is full of surprises.

4375.book Page 9 Monday, October 18, 2004 3:13 PM

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 a law enforcement agent asks you to do something, you can be bound by the same restrictions that they encounter. 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.

Both law enforcement and corporate practitioners are guided by a set of *best practices* set forth by various agencies. In the law enforcement arena, a set of best practices exists for electronic discovery and how to properly retrieve data. The corporate world has established best practices for security and best practices for determining what comprises an *incident*. These best practices iterate *incident response* procedures regarding how to react to an incident. Because disasters are usually of a larger magnitude, best practices for *disaster recovery* may affect both. The focus of this book is to provide information that can be used in either discipline and not geared specifically toward law enforcement.

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.

Corporate Concerns Focus on Detection and Prevention

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. For example, an article from Silicon.com reported that during the first quarter of 2003, the number of security events detected by companies jumped 84 percent over the preceding three months. 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 the worm had been 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 a court of law.

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 having *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 the procedures for investigations, including the when, who, and how in regard to contacting law enforcement.

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

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.

4375.book Page 10 Monday, October 18, 2004 3:13 PM

virus
A program or piece of code that is loaded onto your computer without your knowledge and is designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched.

worm
Similar in function and behavior to a virus, with the exception 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.

Companies can access websites 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.

You'll find in many corporate environments that incidents are not reported, often times 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 the management responsible for data breaches. A company is potentially liable for damages caused by a hacker 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 was enacted to ensure that only patients and their healthcare 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 healthcare institutions and individuals who disclose confidential health information.

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. Among other institutions, it includes check-cashing businesses, mortgage brokers, real estate appraisers, professional tax prepares, 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 making chief executives of publicly traded companies personally validate financial statements and other information. Congress passed the law to avoid future accounting scandals such as those committed by Enron and WorldCom. The law was signed on July 30, 2002. Large corporations must be in compliance by June 15, 2004, and smaller companies have to comply by April 15, 2005. The executives who have to sign off on the 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," it will be viewed as a sign of noncompliance.

Often, the victim company 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 the Federal Bureau of Investigation (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

4375.book Page 11 Monday, October 18, 2004 3:13 PM

seriously jeopardize the normal operations of a company, not only for the customers but for the employees as well. The interruption to the workplace causes confusion and disrupts employee schedules. Furthermore, cases are often hard to pursue if the suspect is a juvenile or the intruder is from another country, and in many states the amount of damage inflicted by the intruder is too small to justify prosecution. Lastly, pursuing such matters can take a long time and be costly.

Many businesses perceive that there is little upside to reporting network intrusions.

NOTE

Law Enforcement Focuses on 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 can be prosecuted. For cases to be prosecuted, evidence must be properly collected, processed, and preserved. In later chapters, we'll go through these processes. Technology has dramatically increased the universe of discoverable electronic material, thereby making the job of law enforcement much more complicated. 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.

Law enforcement must deal with incredible amounts of data. When the Internet is involved, crimes can be committed from other states and countries, thereby involving the laws and jurisdiction of those locales. The following high-profile case about hackers from Russia is a perfect example of this situation.

Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies

On June 20, 2001, a federal grand jury indicted a computer hacker on several federal charges for allegedly accessing computer systems owned by several companies, stealing credit card information, and requesting payments for computer security services from the companies. Alexey V. Ivanov, of Chelyabinsk, Russia, was charged with four counts of unauthorized computer intrusions, eight counts of wire fraud, two counts of extortion, and one count of possessing usernames and passwords for an online bank. Ivanov allegedly used one of the stolen credit card numbers to open an account with CTS Network Services, an Internet service provider in San Diego. He then hacked into CTS computers and used them to launch attacks against other e-commerce companies.

To obtain evidence for the case, the FBI set up a sting operation in which it advertised a job offer for a fictitious company named Invita Security, Inc., which drew Ivanov and his partner, 25-year-old Vasili Gorchkov, to the United States.

4375.book Page 12 Monday, October 18, 2004 3:13 PM

During the sting operation, the two men were invited to log on to their computer in Russia from the Invita offices. FBI agents captured the keystroke information, which they used to access the Russian's computer over the Internet and download its data. However, the FBI agents did not contact Russian law enforcement officials, thus violating Russian Criminal Code Article 272 that punishes "unlawful access to computer information" with up to two years in prison. The U.S. federal judge presiding over the case ruled that the downloaded evidence was admissible in court, finding that the FBI wasn't subject to Russian law. Gorchkov was subsequently convicted of 20 counts of wire fraud.

NOTE

Source: U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), `http://www.usdoj.gov/criminal/cybercrime/ivanovIndict2.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's 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 having profound impact in many cases. Courts are generally not persuaded by the authenticity, best evidence rule, chain of custody, and other challenges to the introduction of electronic data 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 the authenticity of the 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 ones that are violent usually get high priority along with crimes that result in large monetary loss.

Crime Jurisdiction Crimes that affect the locale 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 to investigate.

4375.book Page 13 Monday, October 18, 2004 3:13 PM

Availability and Training of Personnel Often crimes that don't require a large amount of manpower or very specific training may 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 website is located at `http://htcia.org`. The website includes links to chapters throughout the world, which include information on local laws associated with computer crimes.

Training

To effectively fight cybercrime, everyone who deals with it must be educated. This includes the criminal justice and the IT communities, as well as the everyday user. Imagine what would happen to evidence if a law enforcement officer wasn't properly trained and, as a result of his actions, a good portion of evidence was destroyed. Many times, the judge or jury does not understand the topics discussed or lack the technical expertise to interpret the law. What would happen in a complex case if the jury, prosecutor, and the judge had little experience with computers? 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 so than that of child pornography. Child pornography issues present circumstances in which the prosecution might have to prove that a photograph is one of a real child due to rulings on virtual pornography. 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 that you want to fill so that you get the most benefit. Here are some common roles that could involve the process of 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 employers for both the corporate and law enforcement worlds and the type of training available for them.

Practitioners

Civil litigators can utilize personal and business computer records in cases involving fraud, divorce, and harassment. Insurance companies might be able to

4375.book Page 14 Monday, October 18, 2004 3:13 PM

reduce costs by using computer evidence of possible fraud in accident, arson, and workman's compensation cases. Corporations hire computer forensics specialists to obtain evidence relating to embezzlement, theft, and misappropriation of trade secrets. Individuals sometimes hire computer forensic specialists in support of claims for wrongful termination, sexual harassment, and age discrimination.

Law enforcement officials sometimes require assistance in pre-search warrant preparations and post-seizure handling of the computer equipment. Criminal and civil proceedings often use evidence revealed by computer forensics specialists. Criminal prosecutors use computer evidence in cases such as financial fraud, drug and embezzlement record-keeping, and child pornography.

All these various types of industries rely on properly trained computer forensics investigators. The following sections describe some of the training available to both the corporate and law enforcement worlds. The role that you will 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. In other words, legislators need to understand the laws that are proposed and that they are passing, whereas 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. They should know how to recover data, read log files, and decrypt data. 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 ideas on getting the training needed to pursue a career in computer forensics:

- Intense School's CCE Applied Computer Forensics Boot Camp: `http://www.intenseschool.com/bootcamps/default.asp`
- NTI's computer forensics and security training: `http://www.forensics-intl.com/training.html`
- WorldWide Learn's Computer Forensic Training Center Online: `http://www.worldwidelearn.com/keycomputer/forensic-training.htm`
- Mares and Company, LLC's basic and advanced computer forensic training: `http://www.dmares.com/maresware/training.htm`
- AccessData's computer forensic courses: `http://www.accessdata.com/training/viewclasses.php`
- DIBS computer forensic training courses: `http://www.dibsusa.com/training/training.html`

4375.book Page 15 Monday, October 18, 2004 3:13 PM

Many local community colleges 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), which is online at `http://www.cops.org/`.

New Technologies Inc. (NTI) also makes training films concerning computer evidence processing and computer security topics available to government agencies, law enforcement agencies, and businesses. The selection of training films is listed on NTI's Computer Forensics Information and Reference Page.

Corporate

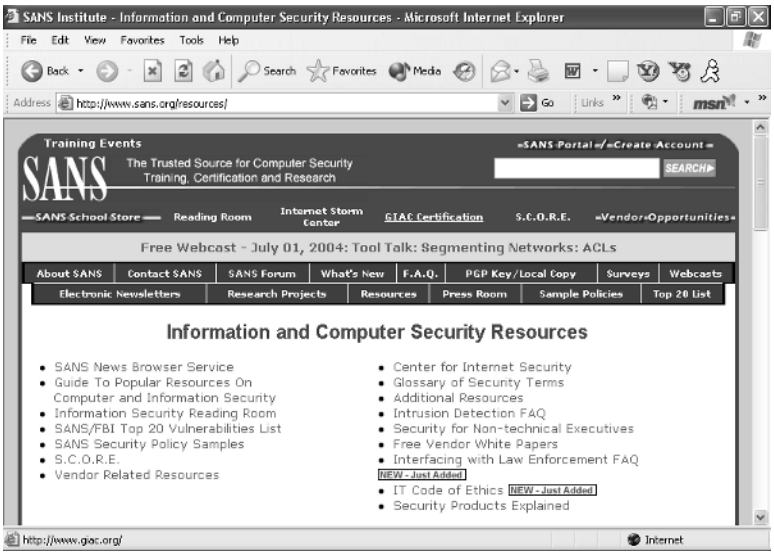
Frequently, security and disaster recovery projects aren't funded because they don't produce revenue. An Ernst & Young annual security survey of 1,400 organizations states that only 13 percent think that spending money on IT training is a priority. This shows that training is needed not only for IT professionals 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. In order 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 that is 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 be trained on how laws are made, how crimes are investigated, and how crimes are prosecuted. This training could 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) website at `http://www.sans.org`. 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. The graphic on the following page shows the SANS Information and Computer Security Resources webpage.

End Users

Legislation such as Sarbanes-Oxley will not change behaviors simply because it is law. This is similar to speeding. Laws against driving over a certain speed do not stop

4375.book Page 16 Monday, October 18, 2004 3:13 PM



some people from speeding. In fact, 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 the organization's principles and values. As mentioned previously, management must be trained and become an integral part of the education and training process in order for the users to buy into it.

WARNING

The hardest environment to control is that of the end user. Training and education are vital parts of any organization that has computer users or Internet access.

Security Awareness

malware
Another name for malicious code. This includes viruses, logic bombs, and worms.

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, the network can be jeopardized in one phone call or click of a button if users aren't taught the dangers of social engineering, e-mail scams, and *malware*.

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 the password would eliminate a lot of effort on your part. Social engineering is hard to detect because you have very little influence over lack of common sense or ignorance on the part of employees, but education should help eliminate ignorance. Most business environments are fast paced and service oriented. Human nature is trusting and often naïve.

4375.book Page 17 Monday, October 18, 2004 3:13 PM

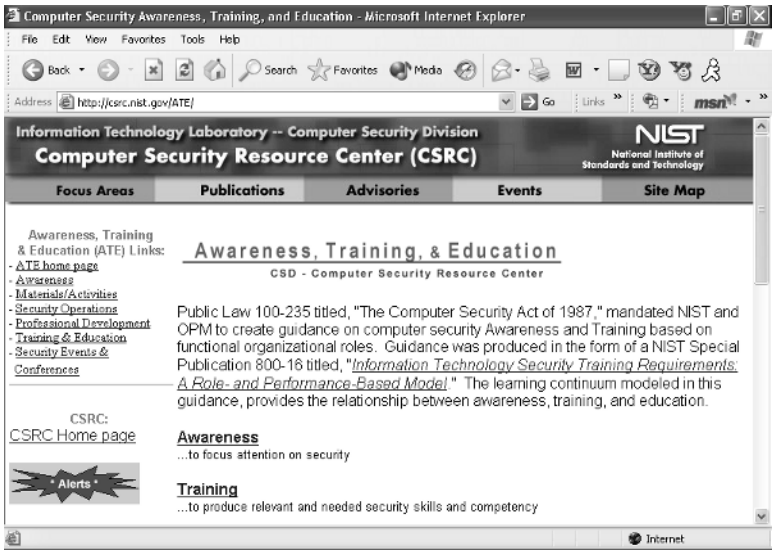
Take this scenario for example. A vice president calls the help desk and states that he's in real trouble. He's trying to present a slideshow to an important client and has forgotten his password; therefore, he can't log onto the company website to run the presentation. He changed the password yesterday and can't remember what the new one is. He needs it right away because a room full of people are 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, he could be giving it to an intruder.

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

When creating a security-awareness program, organizations should have 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.

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), as shown in the following graphic.



4375.book Page 18 Monday, October 18, 2004 3:13 PM

If you can't educate your employees yourself, make sure you set up training for them either in-house or with outside vendors. Not having the time to train them yourself is no excuse for not training employees at all.

How Much Is Actually Monitored?

Security experts have the capability to monitor vast amounts of data. They can track Internet access, read employee e-mail messages, record phone calls, and monitor network access. All this monitoring creates a large amount of data. How much you should monitor depends on how much information you want to store. Keep in mind 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. The following are some items to consider when you are ready to implement a monitoring policy:

- Identify potential resources at risk within your environment (for example, sensitive files, financial applications, and personnel files).
- After the resources are identified, set up the policy. If the policy requires auditing large amounts of data, make sure that the hardware has the additional space needed, as well as processing power and memory.
- Make time to view the logs. The information in the log files won't help protect against a system compromise if you don't read it for six months.

NOTE

You can monitor as much or as little as you want, but if you don't read the logs, they are not serving their purpose.

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.

What Are Your Organization's Needs?

Each organization has different needs. 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 factor to determine how best to keep their networking environment safe. Corporations can also have outdated equipment or applications, making their networks more vulnerable.

4375.book Page 19 Monday, October 18, 2004 3:13 PM

Because every organization is different, with different policies and requirements, there are no "one size fits all" rules to ensure all security bases are covered. Training and education will make a good start, but you must constantly update your knowledge of new 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.

Terms to Know

backdoor
best practices
computer forensics
disaster recovery
electronic discovery
incident
incident response
intrusion detection
logic bomb
malware
security policies
social engineering
virus
worm

4375.book Page 20 Monday, October 18, 2004 3:13 PM

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. What is the difference between a virus and a worm?
7. Why aren't incidents in many corporate environments reported?
8. What law was passed to avoid future accounting scandals such as those involving Enron and WorldCom?
9. Name some factors that will determine which criminal cases get priority.
10. Name a good resource for computer forensics training for law enforcement.