chapter 1

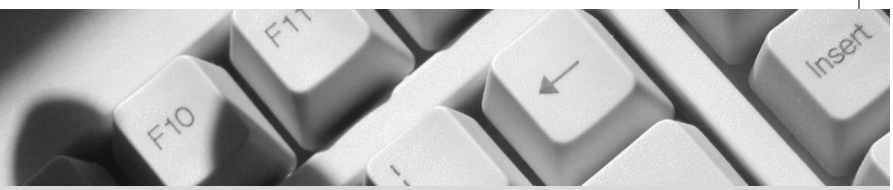
# Introduction to Security



## After completing this chapter, you will be able to do the following:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- List the basic steps of an attack
- Describe the five basic principles of defense

## Today's Attacks and Defenses




*"Groundbreaking," "amazing," "never seen before," "extremely impressive," "clever," "something out of a movie," "scary," "the most sophisticated malware ever," "other attacks are child's play compared to it…."* These are just a few of the adjectives security researchers used to describe the Stuxnet malware.

The Stuxnet worm was first widely reported in mid-2010, although it's now thought that it first appeared almost a year earlier. Shortly after it became widely recognized, Microsoft confirmed the worm was actively targeting Windows computers that managed large-scale industrial-control systems, which are often referred to as SCADA (*Supervisory Control and Data Acquisition*). SCADA can be found in military installations, oil pipeline control systems, manufacturing environments, and nuclear power plants. At first, it was thought that Stuxnet took advantage of a single, previously unknown, software vulnerability. Upon closer inspection, it was found that Stuxnet exploited *four* unknown vulnerabilities, something never seen before. (One of these vulnerabilities was "patched" in 2008 by Microsoft, but the fix was flawed and could still be exploited.)

Stuxnet, written in multiple languages, including C, C++, and other object-oriented languages, was introduced to industrial networks through infected Universal Serial Bus (USB) flash drives. It also used several tricks to avoid detection. Stuxnet had an internal counter that allowed it to spread to a maximum of three computers. This design ensured that it stayed only within the industrial facility and didn't attract outside attention. Also, because SCADA systems have no logging capabilities to record events and are rarely patched, the worm could live for a long period of time before being detected.

Using Windows vulnerabilities, Stuxnet performed an attack to gain administrative access to computers on the local network of an industrial plant and then looked for computers running SCADA. Next, it infected these SCADA computers—through two other vulnerabilities—and tried to break into the SCADA software by using the default passwords. Stuxnet was designed to alter the programmable logic control (PLC) software instructions of the SCADA systems, which would then give it power over the industrial machinery attached to the SCADA computers. This would put the entire facility under the control of the attacker, who could make the equipment operate in an unsafe manner, resulting in a massive explosion or even worse, a nuclear catastrophe.

It is speculated that Stuxnet's primary target was the Iranian Bushehr nuclear power plant (almost six out of ten infected Stuxnet computers have been traced back to Iran). This reactor, located in southwestern Iran near the Persian Gulf, has been a source of tension between Iran and the West (including the United States) because of fear that

*(continued)*

spent fuel from the reactor could be reprocessed elsewhere in the country to produce weapons-grade plutonium for use in nuclear warheads. Some have even speculated that an unnamed government-sponsored team of programmers—or even teams from multiple opposition governments—created Stuxnet to cripple the Bushehr facility. Based on the complexity of the software, it is estimated that the cost for developing Stuxnet could have exceeded $4 million.

As far as can be determined, Stuxnet never did gain control of any SCADA systems or cause damage to industrial sites. No person or organization has yet stepped forward as the author of Stuxnet, so it remains cloaked in secrecy. Although we may not know who was behind it and why, Stuxnet is just one example of how extremely dangerous malicious software can be.



When historians reflect back on the early part of the twenty-first century, it is likely that one word will figure prominently: *security*. At no other time in the world's history have we been forced to protect ourselves and our property from continual attacks by invisible foes. Suicide car bombings, subway massacres, airplane hijackings, random shootings, and guerrilla commando raids occur regularly around the world. To counteract this violence, governments and other organizations have implemented new types of security defenses. Passengers using public transportation are routinely searched. Fences are erected across borders. Telephone calls are monitored. The result is that these attacks and the security defenses have impacted almost every element of our daily lives and significantly affect how all of us work, play, and live.

One area that has also been an especially frequent target of attacks is information technology (IT). Seemingly endless arrays of attacks are directed at corporations, banks, schools, and individuals through their computers, laptops, smartphones, pad computers, and similar technology devices. Internet Web servers must resist thousands of attacks daily. Identity theft has skyrocketed. An unprotected computer connected to the Internet can be infected in less than one minute. One study found that over 48 percent of 22.7 million computers analyzed were infected with malware.[1] Phishing, rootkits, back doors, social engineering, zombies, and botnets—virtually unheard of just a few years ago—are now part of our everyday information security vocabulary.

The need to defend against these attacks on our technology devices has created a new element of IT that is now at the very core of the entire industry. Known as *information security,* it is focused on protecting the electronic information of organizations and users.

The demand for IT professionals who know how to secure networks and computers is at an all-time high. Today, many businesses and organizations require employees as well as job applicants to demonstrate that they are familiar with computer security practices. To verify security competency, a vast majority of organizations use the CompTIA Security+ certification. As the most widely recognized vendor-neutral security certification, Security+ has become the security foundation for today's IT professionals.

There are two broad categories of information security positions. Information security managerial positions include the administration and management of plans, policies, and people. Information security technical positions are concerned with the design, configuration,

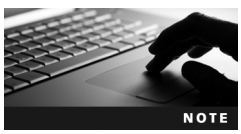
installation, and maintenance of technical security equipment. Within these two broad categories, there are four generally recognized security positions:

- *Chief Information Security Officer (CISO)*. This person reports directly to the CIO (large organizations may have more layers of management for reporting). Other titles used are Manager for Security and Security Administrator. They are responsible for the assessment, management, and implementation of security.
- *Security manager*. The security manager reports to the CISO and supervises technicians, administrators, and security staff. Typically, a security manager works on tasks identified by the CISO and resolves issues identified by technicians. This position requires an understanding of configuration and operation but not necessarily technical mastery.
- *Security administrator*. The security administrator has both technical knowledge and managerial skills. A security administrator manages daily operations of security technology, and may analyze and design security solutions within a specific entity as well as identify users' needs.
- *Security technician*. This is generally an entry-level position for a person who has the necessary technical skills. Technicians provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems.

Recent employment trends indicate that employees with security certifications are in high demand. As attacks continue to escalate, the need for trained security personnel also increases. Unlike some positions, security is being neither offshored nor outsourced. Because security is such a critical element in an organization, security positions generally remain within the organization. In addition, security positions do not involve "on-the-job training" where a person can learn as they go; the risk is simply too great. IT employers want and pay a premium for certified security personnel.


A study by Foote Partners showed that security certifications will earn employees 10 to 14 percent more pay than their uncertified counterparts.[2]

The CompTIA Security+ Certification is a vendor-neutral credential that requires passing the current certification exam SY0-301. This exam is internationally recognized as validating a foundation-level of security skills and knowledge. A successful candidate has the knowledge and skills required to identify risks and participate in risk mitigation activities; provide infrastructure, application, operational and information security; apply security controls to maintain confidentiality, integrity, and availability; identify appropriate technologies and products; and operate with an awareness of applicable policies, laws, and regulations.




The CompTIA Security+ Certification is aimed at an IT security professional with the recommended background of a minimum of two years experience in IT administration with a focus on security. Such a professional is involved with daily technical information security experience, and has a broad knowledge of security concerns and implementation.

1

This chapter introduces network security fundamentals that form the basis of the Security+ certification. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail and explores why it is important. Finally, the chapter looks at who is responsible for these attacks and at the fundamental defenses against attackers.



# Challenges of Securing Information

Although to a casual observer it may seem that there should be a straightforward solution to securing computers—such as using a better software product or creating a stronger password—in reality, there is no simple solution to securing information. This can be seen through the different types of attacks that users face today as well as the difficulties in defending against these attacks.

## Today's Security Attacks

Despite the facts that information security continues to rank as the number one concern of IT managers and tens of billions of dollars are spent annually on computer security, the number of successful attacks continues to increase. Information regarding recent attacks includes the following:

- Fake anti-virus attacks are responsible for half of all malware delivered by Web advertising, which increased 500 percent in one 12-month period. Over 11,000 domains are involved with fake anti-virus distribution, and that number is increasing.[3] In one example, a user who clicks an advertisement on a Web page offering a free online vulnerability scan suddenly sees a window that informs the user that the computer is infected. The pop-up window directs the user to click a button to purchase anti-virus software to disinfect their computer. However, this window cannot be closed, and even rebooting the system does not clear the message. In desperation, many users finally enter their credit card number to purchase the anti-virus software. Their credit card number is then transmitted to an attacker, who uses it to make online purchases. At the same time, other malware software is installed on the computer while the pop-up window remains open on the computer and never goes away.
- Approximately 80 percent of households in the United States use the Internet for managing their finances, up from only 4 percent just 15 years ago. And the trend is toward even more online banking. There are now Internet-only banks, with no physical branches to visit. One new bank is planning to limit its membership to smartphone users (although these users can access their account information from their computers as well). Yet the number of malware attacks against online banking is increasing annually by almost 60,000. About 85 percent of banks reported that they have sustained losses based on these attacks. The American Bankers Association says that consumers should monitor their online accounts for unauthorized transactions on a "continuous, almost daily, basis."[4]
- A graphics processing unit (GPU), which is separate from the computer's central processing unit (CPU), is used in graphics cards to render screen displays on

computers. Today, some of the work of a CPU can be offloaded to a GPU to accelerate specific applications, most notably floating-point operations. A $500 GPU today can process about 2 trillion (teraflop) floating-point operations per second, whereas just 10 years ago, the fastest supercomputer in the world only ran at 7 teraflops and cost $110 million. Attackers are now using GPUs to break passwords. Researchers at the Georgia Tech Research Institute (GTRI) claim that an attacker with a computer that has a GPU could easily break a relatively weak password. They state, "Right now we can confidently say that a 7-character password is hopelessly inadequate." They go on to say that any password with fewer than 12 characters could be vulnerable very soon—if it is not already.[5]

- According to a security report by IBM's X-Force, on average, 55 percent of software vulnerabilities that were disclosed by vendors were not patched, which is an increase from the previous year's 52 percent. The top ten vendors with the most disclosed yet unpatched vulnerabilities were Sun Microsystems (24%), Microsoft (23.2%), Mozilla (21.3%), Apple (12.9%), IBM (10.3%), Google (8.6%), Linux (8.2%), Oracle (6.8%), Cisco (6%), and Adobe (2.9%).[6]
- Over 135 employees at 17 of the Fortune 500 companies (including Google, WalMart, Symantec, Cisco, Microsoft, Pepsi, Coca-Cola, and Ford) were called on the phone by individuals participating in a Defcon Hacking Conference contest. The callers tried to get information from these employees that could be used in an attack. Callers could not ask for passwords or Social Security numbers, but they tried to find out information that could be useful to attackers, such as what operating system, anti-virus software, and browser their victims used. In addition, they also tried to persuade these employees to visit unauthorized Web pages. Of the 135 employees who were called, only five refused to provide any corporate information or visit the unauthorized Web sites (and all five were women).[7]
- An immigrant pretending to be "Prince Nana Kamokai of Sierra Leone" or "an airport director from Ghana" sent thousands of e-mails asking for help in moving money from Nigeria to the United States. By using fake documentation to convince his victims that he was legitimate, he persuaded them to wire him fees to cover "courier services" or as "PIN code fees." After five years, he had made more than $1.3 million from 67 known victims. Yet this was only a drop in the bucket for this scam, known as the Nigerian 419 Advanced Fee Fraud ("419" is the Nigerian criminal code that addresses fraud). To date, it is estimated that over $41 billion dollars have been lost by victims in this scam, with $9.3 billion lost in 2009 alone. According to the U.S. Federal Bureau of Investigation (FBI), this scam is the number-one type of Internet fraud and is growing at a rate of 5 percent annually.[8]
- Firesheep is a free, open-source Firefox browser extension introduced in late 2010. An attacker can install this add-on and then connect to an unencrypted wireless network at a coffee shop, hotel, or library. Once the attacker clicks Start Capturing, then anyone using the wireless network who visits a site that is known by Firesheep (such as Facebook, Twitter, Amazon, FourSquare, Dropbox, Windows Live, WordPress, or Flickr) will have their name and even their photo displayed. The attacker can then double-click the name and be logged in as that person to that account.

- According to Panda Security, over 20 million new specimens of malware, including new malware as well as variants of existing families, were created between January and October of 2010. This means that the average number of new threats created and distributed every day increased from 55,000 in 2009 to 63,000 in 2010. In one month, over 2 million files were identified as malware.[9]
- An analysis of 700,000 recorded attacks on computers in one week revealed that about one out of every eight attacks came by USB flash drive devices.[10] A user's USB device may become infected at home where they have less security. When they bring the infected device into the office to insert into their work computer, that computer is then infected. In addition, attackers leave infected USB flash drives in parking lots and other common areas outside an office, tempting users to pick them up on the way to their office and to insert them into their computers.
- Two former students at a college in Missouri were indicted on a series of charges for breaking into the school's computers. These students (1) stole personal data on 90,000 students, faculty, staff, and alumni and tried to sell it for $35,000; (2) obtained the username and password of a residence hall director to access a university computer and then on 30 different occasions transferred university funds (from $50 to $4,300) to their own student accounts; (3) used their Facebook accounts to threaten potential witnesses; and (4) created a virus and infected other university computers that allowed them to monitor activity, record keystrokes, steal data, and even remotely turn on the computers' webcams to watch users.[11]
- In late 2010, Apple released patches to address 134 security flaws (in March 2010, it released patches to fix 90 flaws) in its Leopard and Snow Leopard Mac OS X. An additional 25 nonsecurity fixes addressed stability issues. The patch was between 240 MB and 645 MB, depending on the version of Mac OS X.[12]
- Researchers at the University of Maryland attached four computers equipped with weak passwords to the Internet for 24 days to see what would happen. These computers were hit by an intrusion attempt on average once every 39 seconds, or 2,244 attacks each day for a total of 270,000 attacks. Over 825 of the attacks were successful, enabling the attackers to access the computers.[13]
- In 2010, smartphones outsold computers for the first time (421 million smartphones to 365 million personal computers). With the proliferation of smartphones, which are essentially mobile computing devices, attackers are turning their attention to them. The mobile-security company Lockout reported that it detected malware on 9 percent of the smartphones that it had scanned.[14]
- The number of security breaches that have exposed users' digital data to attackers continues to rise. Table 1-1 lists some of the major security breaches that occurred during a one-month period, according to the Privacy Rights Clearinghouse. From January 2005 through February 2011, over 514 million electronic data records in the United States had been breached, exposing to attackers a range of personal electronic data, such as addresses, Social Security numbers, health records, and credit card numbers. [15]

Security attacks continue to be a major concern of all IT users, especially those personnel responsible for protecting an organization's information.

| Organization | Description of security breach | Number of identities exposed |
|---|---|---|
| Grays Harbor Pediatrics, WA | A backup tape, stolen from an employee's car, was used for storing copies of paper records; patients may have had their names, Social Security numbers, insurance details, driver's license information, immunization records, medical history forms, previous doctor records, and patient medical records stolen | 12,000 |
| Tulane University, LA | A university-issued laptop was stolen from an employee's car. It was used to process 2010 tax records for employees, students, and others; the information included names, Social Security numbers, salary information, and addresses | 10,000 |
| Seacoast Radiology, NH | Patient names, Social Security numbers, addresses, phone numbers, and other personal information were exposed by a security breach | 231,400 |
| Centra, GA | A laptop was stolen from the trunk of an employee's rental car that contained patient names and billing information | 11,982 |
| Stony Brook University, NY | Student and faculty network and student IDs were posted online after a file with all registered student and faculty ID numbers was exposed | 61,001 |
| deviantART, Silverpop Systems Inc., CA | Attackers exposed the e-mail addresses, usernames, and birth dates of the entire user database | 13,000,000 |
| Twin America LLC, CitySights, NY | An attacker inserted a malicious script on a Web server and stole the customer database that contained customer names, credit card numbers, credit card expiration dates, CVV2 data, addresses, and e-mail addresses | 110,000 |
| Ohio State University, OH | Unauthorized individuals logged into an Ohio State server and accessed the names, Social Security numbers, dates of birth, and addresses of current and former students, faculty, staff, University consultants, and University contractors | 750,000 |
| Gawker, NY | Attackers gained access to the database and accessed staff and user e-mails and passwords | 1,300,000 |

**Table 1-1** Selected security breaches involving personal information in a one-month period

## Difficulties in Defending Against Attacks

The challenge of keeping computers secure has never been greater, not only because of the number of attacks, but also because of the difficulties faced in defending against these attacks. These difficulties include the following:

- *Universally connected devices.* It is virtually unheard of today for a computer to not be connected to the Internet. Although this greatly expands the functionality of that device, it also makes it easy for an attacker halfway around the world to silently launch an attack on any connected device.
- *Increased speed of attacks.* With modern tools at their disposal, attackers can quickly scan thousands of systems to find weaknesses and launch attacks with unprecedented speed. Many tools can even initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.

- *Greater sophistication of attacks.* Attacks are becoming more complex, making it more difficult to detect and defend against them. Attackers today use common Internet tools and protocols to send malicious data or commands to strike computers, making it difficult to distinguish an attack from legitimate traffic. Other attack tools vary their behavior so the same attack appears differently each time, further complicating detection.
- *Availability and simplicity of attack tools.* Whereas in the past an attacker needed to have an extensive technical knowledge of networks and computers as well as the ability to write a program to generate the attack, that is no longer the case. Today's attack tools do not require any sophisticated knowledge. In fact, many of the tools have a graphical user interface (GUI) that allows the user to select options easily from a menu, as seen in Figure 1-1. These tools are freely available or can be purchased from other attackers at a low cost. This is illustrated in Figure 1-2.

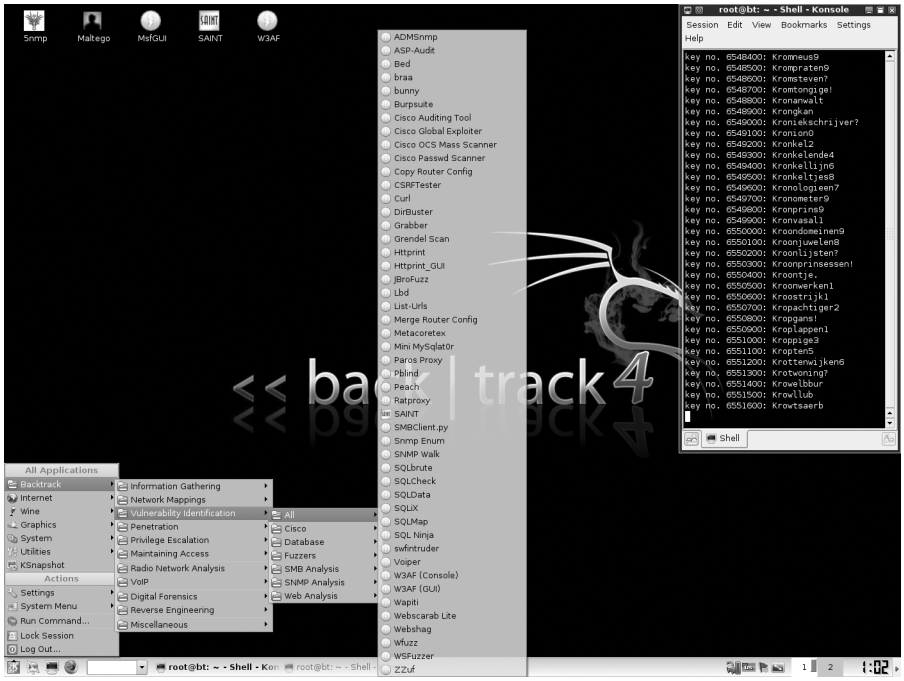



**Figure 1-1** Menu of attack tools



- *Faster detection of vulnerabilities.* Weakness in software can be more quickly uncovered and exploited with new software tools and techniques.
- *Delays in patching.* Hardware and software vendors are overwhelmed trying to keep pace with updating their products against attacks. One anti-virus software vendor receives over 200,000 submissions of potential malware each month.[16] At this rate, the anti-virus vendors would have to update and distribute their updates *every 10 minutes* to keep users protected. The delay in vendors patching their own products adds to the difficulties in defending against attacks.

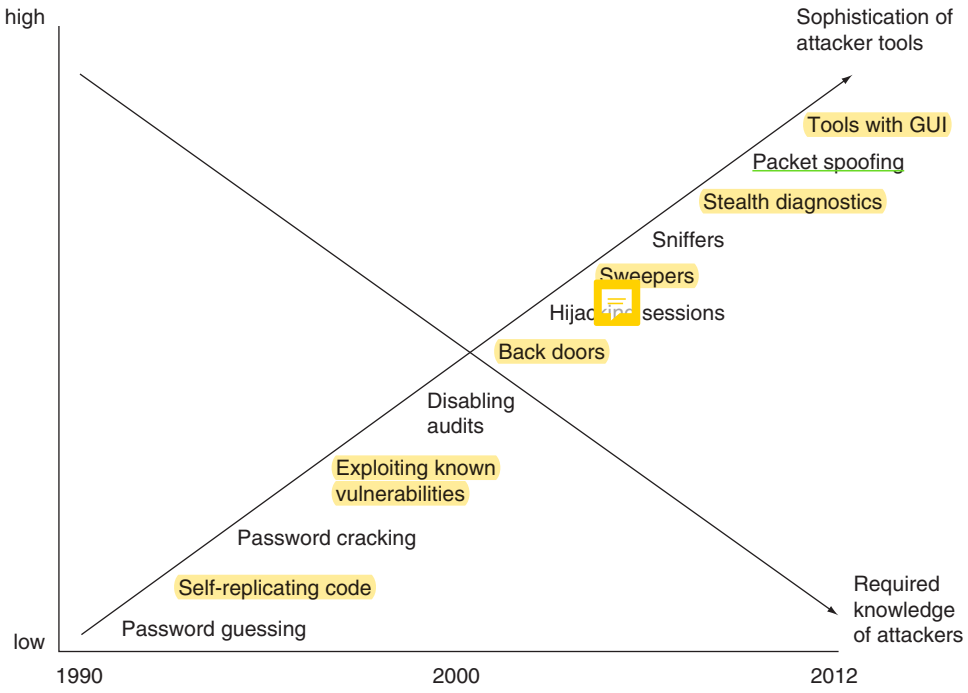



**Figure 1-2** As the sophistication of attack tools increases, the knowledge required by attackers decreases



- *Weak patch distribution.* While mainstream products such as Microsoft Windows and Apple Mac OS have created a system for notifying users of patches and distributing those patches on a regular basis, other software vendors have not invested in distribution systems. Users are unaware that a security update even exists for a product, and usually it requires downloading and installing the latest version of the product instead of only installing a smaller patch. For these reasons, attackers today are focusing more on uncovering and exploiting vulnerabilities on these products.
- *Distributed attacks.* Attackers can use tens of thousands of computers under their control in an attack against a single server or network. This "many against one" approach makes it virtually impossible to stop an attack by identifying and blocking a single source.
- *User confusion.* Increasingly, users are called upon to make difficult security decisions regarding their computer systems, sometimes with little or no information to guide them. It is not uncommon for a user to be asked security questions such as, *Do you want to view only the content that was delivered securely?, Is it safe to quarantine this attachment?,* or *Do you want to install this add-on?* With little or no direction, users are inclined to provide answers to questions without understanding the security risks.

Table 1-2 summarizes the reasons it is difficult to defend against today's attacks.

| Reason | Description |
|---|---|
| Universally connected devices | Attackers from anywhere in the world can send attacks |
| Increased speed of attacks | Attackers can launch attacks against millions of computers within minutes |
| Greater sophistication of attacks | Attack tools vary their behavior so the same attack appears differently each time |
| Availability and simplicity of attack tools | Attacks are no longer limited to highly skilled attackers |
| Faster detection of vulnerabilities | Attackers can discover security holes in hardware or software more quickly |
| Delays in patching | Vendors are overwhelmed trying to keep pace by updating their products against attacks |
| Weak patch distribution | Many software products lack a means to distribute security patches in a timely fashion |
| Distributed attacks | Attackers use thousands of computers in an attack against a single computer or network |
| User confusion | Users are required to make difficult security decisions with little or no instruction |

**Table 1-2** Difficulties in defending against attacks

# What Is Information Security?


2.8 Exemplify the concepts of confidentiality, integrity and availability (CIA)

3.2 Analyze and differentiate among types of attacks

5.2 Explain the fundamental concepts and best practices related to authentication, authorization and access control

Before it is possible to defend computers against attacks, it is necessary to understand what information security is. In addition, knowing why information security is important today and who the attackers are is beneficial.

## Defining Information Security

In a general sense, *security* may be defined as the necessary steps to protect a person or property from harm. That harm may come primarily from two different sources:

- A direct action that is intended to inflict damage or suffering.
- An indirect and nonintentional action.

Consider a typical house. It is necessary to provide security for the house and its inhabitants from these two different sources. For example, the house and its occupants must be secure from the direct attack of a criminal who wants to inflict bodily harm to someone inside or who wants to burn down the house. This security may be provided by locked doors, a fence, or a strong police presence. In addition, the house must be protected from indirect acts that are not exclusively

directed against it. That is, the house needs to be protected from a hurricane (by being built with strong materials such as concrete blocks) or a flash flood (by being built off the ground).

Security usually includes preventive measures, rapid response, and in some instances, preemptive attacks. An individual who wants to be secure would take the preventive measures of not walking alone in a risky neighborhood at night and keeping car doors locked. An example of a rapid response could include holding a cell phone in one hand when making a withdrawal at an ATM, so that if anything suspicious begins to occur, an emergency call can quickly be made to the police. Preemptive attacks are sometimes carried out by one nation against another nation that has started to amass troops and equipment along a border. This approach of "strike them before they can strike us" can be used to deter an attack.

The term **information security** is frequently used to describe the tasks of securing information that is in a digital format. This digital information is typically manipulated by a microprocessor (such as on a personal computer), stored on a magnetic, optical, or solid-state storage device (like a hard drive, DVD, or flash drive), and transmitted over a network (such as a local area network or the Internet).


Security may be viewed as *sacrificing convenience for safety.* Although it may be inconvenient to lock all the doors of the house or use long and complex passwords, the trade-off is that these steps result in a higher level of safety. Another way to think of security is *giving up short-term ease for long-term protection.* In any case, security usually requires making sacrifices to achieve a greater good.

Information security can be understood by examining its goals and how it is accomplished. First, information security ensures that protective measures are properly implemented. Just as the security measures taken for a house can never guarantee complete safety, information security cannot completely prevent attacks or guarantee that a system is totally secure. Rather, information security creates a defense that attempts to ward off attacks and prevents the collapse of the system when a successful attack occurs. Thus, information security is *protection*.

Second, information security is intended to protect information that provides value to people and organizations. Three protections must be extended over information. These three protections are confidentiality, integrity, and availability or CIA:

1. *Confidentiality.* It is important that only approved individuals are able to access important information. For example, the credit card number used to make an online purchase must be kept secure and not made available to other parties. **Confidentiality** ensures that only authorized parties can view the information. Providing confidentiality can involve several different tools, ranging from software to "scramble" the credit card number stored on the Web server to door locks to prevent access to those servers.
2. *Integrity.* **Integrity** ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, an attacker who could change the amount of a purchase from $1,000.00 to $1.00 would violate the integrity of the information.
3. *Availability.* Information cannot be "locked up" so tight that no one can access it; otherwise, the information would not be useful. **Availability** ensures that data is accessible to authorized users. The total number of items ordered as the result of an

online purchase must be made available to an employee in a warehouse so that the correct items can be shipped to the customer.

In addition to CIA, another set of protections must be implemented to secure information. These are authentication, authorization, and accounting (AAA):

1. *Authentication.* **Authentication** ensures that the individual is who they claim to be (the *authentic* or genuine person) and not an imposter. A person accessing the Web server that contains a user's credit card number must prove that they are indeed who they claim to be and not a fraudulent attacker. One way authentication can be performed is by the person providing a password that only she knows.
2. *Authorization.* After a person has provided authentication, they are given **authorization**, or the ability to access the credit card number or enter a room that contains the Web server.
3. *Accounting.* **Accounting** provides tracking of events. This may include a record of who accessed the Web server, from what location, and at what specific time.


There is not universal agreement regarding the three elements of AAA. Some consider it *assurance, authenticity,* and *anonymity*, while others see it as *authentication, authorization,* and *access control*.

Yet information security involves more than protecting the information itself. Because this information is stored on computer hardware, manipulated by software, and transmitted by communications, each of these areas must also be protected. The third objective of information security is to protect the integrity, confidentiality, and availability of information *on the devices that store, manipulate, and transmit the information.*

Information security is achieved through a combination of three entities. As shown in Figure 1-3 and Table 1-3, information, hardware, software, and communications are protected in three layers: products, people, and procedures. These three layers interact with each other. For example, procedures enable people to understand how to use products to protect information. Thus, a more comprehensive definition of information security is *that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.*

## Information Security Terminology

As with many advanced subjects, information security has its own set of terminology. The following scenario helps to illustrate information security terms and how they are used.

Suppose that Aiden wants to purchase a new set of rims for his car. However, because several cars have had their rims stolen near his condo, he is concerned about someone stealing his rims. Although he parks the car in the gated parking lot in front of his condo, a hole in the fence surrounding his condo makes it possible for someone to access the parking lot without restriction. Aiden's car and the threats to the rims are illustrated in Figure 1-4.

Aiden's new rims are an **asset**, which is defined as an item that has value. In an organization, assets have the following qualities: they provide value to the organization, they cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources, and they can form part of the organization's corporate identity. Based on these qualities, not all elements of an organization's information technology infrastructure may be classified as

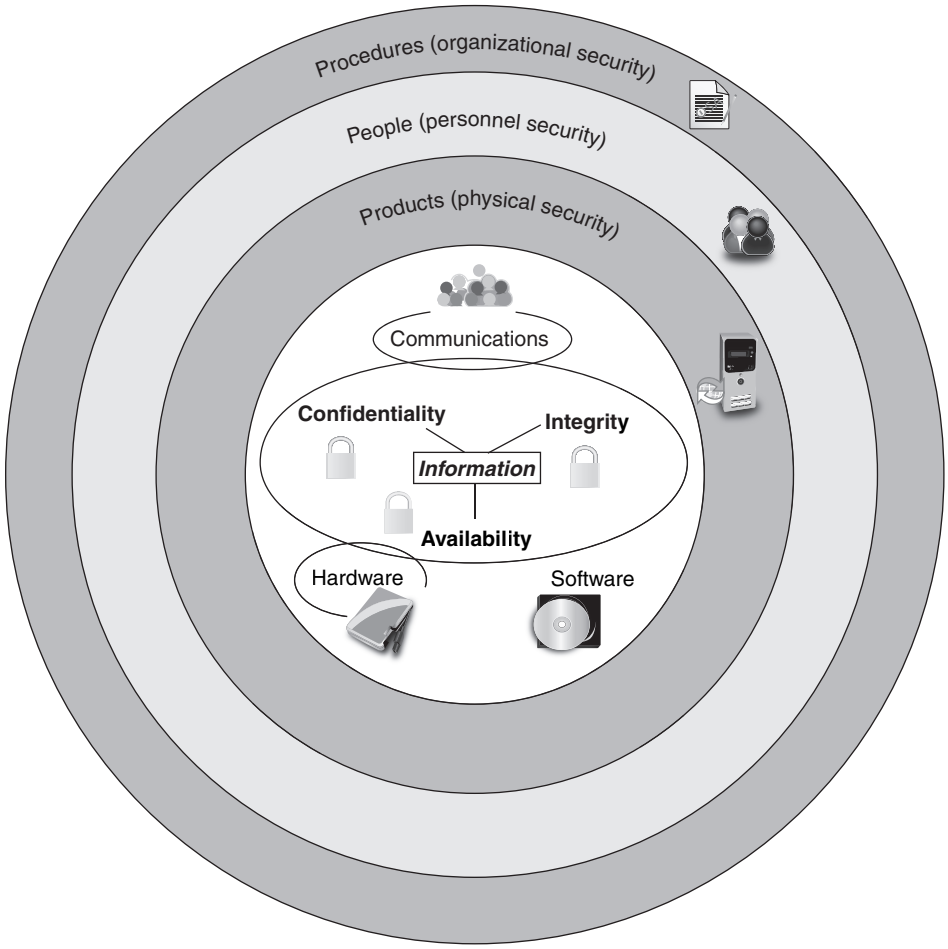



**Figure 1-3** Information security components


| Layer | Description |
|---|---|
| Products | Form the physical security around the data; may be as basic as door locks or as complicated as network security equipment |
| People | Those who implement and properly use security products to protect data |
| Procedures | Plans and policies established by an organization to ensure that people correctly use the products |

**Table 1-3** Information security layers

an asset. For example, a faulty desktop computer that can easily be replaced would generally not be considered an asset, yet the information contained on that computer can be an asset. Table 1-4 lists a description of the elements of an organization's information technology infrastructure and whether or not they would normally be considered as an asset.

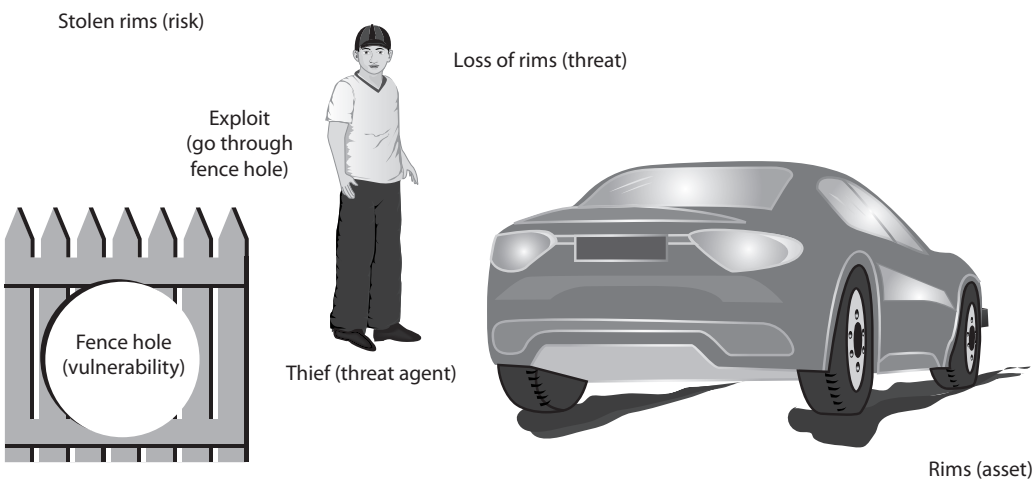



**Figure 1-4** Information security components analogy



| Element name | Description | Example | Critical asset? |
|---|---|---|---|
| Information | Data that has been collected, classified, organized, and stored in various forms | Customer, personnel, production, sales, marketing, and finance databases | Yes: Extremely difficult to replace |
| Application software | Software that supports the business processes of the organization | Customized order transaction application, generic word processor | Yes: Unique and customized for the organization<br>No: Generic off-the-shelf software |
| System software | Software that provides the foundation for application software | Operating system | No: Can be easily replaced |
| Physical items | Computer equipment, communications equipment, storage media, furniture, and fixtures | Servers, routers, DVDs, power supplies | No: Can be easily replaced |
| Services | Outsourced computing services | Voice and data communications | No: Can be easily replaced |

**Table 1-4** Information technology assets


The general question to ask when determining if an IT element is an asset is simply, "If this item were destroyed right now, how difficult would it be to replace?"

What Aiden is trying to protect his rims from is a **threat**, which is a type of action that has the potential to cause harm. Information security threats are events or actions that represent a

danger to information assets. A threat by itself does not mean that security has been compromised; rather, it simply means that the potential for creating a loss is real. Although for Aiden the loss would be the theft of his rims, in information security, a loss can be the theft of information, a delay in information being transmitted, or even the loss of good will or reputation.

A **threat agent** is a person or element that has the power to carry out a threat. For Aiden, the threat agent is a thief. In information security, a threat agent could be a person attempting to break into a secure computer network. It could also be a force of nature such as a tornado or flood that could destroy computer equipment and thus destroy information, or it could be malicious software that attacks the computer network.

Aiden wants to protect his rims and is concerned about a hole in the fencing around his condo. The hole in the fencing is a **vulnerability**, which is a flaw or weakness that allows a threat agent to bypass security. An example of a vulnerability that information security must deal with is a software defect in an operating system that allows an unauthorized user to gain control of a computer without the user's knowledge or permission.

If a thief can get to Aiden's car because of the hole in the fence, then that thief is taking advantage of the vulnerability. This is known as **exploiting** the security weakness. An attacker, knowing that an e-mail system does not scan attachments for a virus, is exploiting the vulnerability by sending infected e-mail messages to its users.

Aiden must decide if the risk of theft is too high for him to purchase the new rims. A **risk** is the likelihood that the threat agent will exploit the vulnerability; that is, that the rims will be stolen. Realistically, risk cannot ever be entirely eliminated as it would cost too much and take too long. Rather, some degree of risk must always be assumed. An organization generally asks, "How much risk can we tolerate?"


Sometimes risk is illustrated as the calculation:
Risk = Threat x Vulnerability x Cost.

There are three options when dealing with risks: accept the risk, diminish the risk, or transfer the risk. In Aiden's case, he could accept the risk and buy the new rims, knowing there is the chance of them being stolen. Or he could diminish the risk by parking the car in a rented locked garage. A third option is for Aiden to transfer the risk to someone else. He can do this by purchasing additional car insurance; the insurance company then absorbs the loss and pays if the rims are stolen. In information security, most risks should be diminished if possible. Table 1-5 summarizes information security terms.

## Understanding the Importance of Information Security

Information security is important to organizations as well as to individuals. The goals of information security are many and include preventing data theft, thwarting identity theft, avoiding the legal consequences of not securing information, maintaining productivity, and foiling cyberterrorism.

### Preventing Data Theft

Security is often associated with theft prevention: Aiden parks his car in a locked garage to prevent the rims from being stolen. The same is true with information security: preventing data from being stolen is often cited by organizations as a

| Term | Example in Aiden's scenario | Example in information security |
|---|---|---|
| Asset | Rims | Employee database |
| Threat | Steal rims from car | Steal data |
| Threat agent | Thief | Attacker, virus, flood |
| Vulnerability | Hole in fence | Software defect |
| Exploit | Climb through hole in fence | Send virus to unprotected e-mail server |
| Risk | Transfer to insurance company | Educate users |

**Table 1-5** Information security terminology

primary goal of information security. Business data theft involves stealing proprietary business information, such as research for a new drug or a list of customers that competitors would be eager to acquire.


According to a recent survey of 800 chief information officers, the companies they represented estimated they lost a combined $4.6 billion worth of intellectual property in one year alone and spent approximately $600 million repairing damage from data breaches.[17]

Data theft is not limited to businesses. Individuals are often victims of data thievery. One type of personal data that is a prime target of attackers is credit card numbers. These can be used to purchase thousands of dollars of merchandise online—without having the actual card—before the victim is even aware the number has been stolen. Reported losses from the fraudulent use of stolen credit card information continue to soar, exceeding $5 billion annually.[18]


The extent to which stolen credit card numbers are available can be seen in the price that online thieves charge each other for stolen card numbers. Because credit card numbers are so readily available, a stolen number can be purchased for as little as $2 per card, although for a card that has a guaranteed limit of over $82,000, the cost of the stolen number is $700. If a buyer wants to use a stolen card number to purchase products online, yet is afraid of being traced through the delivery address, a third-party online thief will make the purchase and forward the goods for a fee starting at only $30.[19]

## Thwarting Identity Theft

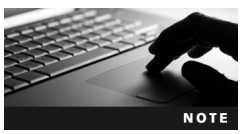
**Identity theft** involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain. The thieves create new bank or credit card accounts under the victim's name. Large purchases are then charged to these accounts that are then left unpaid, leaving the victim responsible for the debts and ruining their credit rating.


In some instances, thieves have bought cars and even houses by taking out loans in someone else's name.

The costs to individuals who have been victims of identity theft as a result of data breaches are significant. A study by Utica College's Center for Identity Management and Information Protection (CIMIP) revealed that the median actual dollar loss for identity theft victims was $31,356.[20]

**Avoiding Legal Consequences** Several federal and state laws have been enacted to protect the privacy of electronic data. Businesses that fail to protect data they possess may face serious financial penalties. Some of these laws include the following:

- *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Under the **Health Insurance Portability and Accountability Act** (**HIPAA**), health care enterprises must guard protected health information and implement policies and procedures to safeguard it, whether it be in paper or electronic format. Those who wrongfully disclose individually identifiable health information with the intent to sell it can be fined up to $250,000 and spend 10 years in prison.
- *The Sarbanes-Oxley Act of 2002 (Sarbox)*. As a reaction to a rash of corporate fraud, the **Sarbanes-Oxley Act** (**Sarbox**) is an attempt to fight corporate corruption. Sarbox covers the corporate officers, auditors, and attorneys of publicly traded companies. Stringent reporting requirements and internal controls on electronic financial reporting systems are required. Corporate officers who willfully and knowingly certify a false financial report can be fined up to $5 million and serve 20 years in prison.
- *The Gramm-Leach-Bliley Act (GLBA)*. Like HIPAA, the **Gramm-Leach-Bliley Act** (**GLBA**) passed in 1999 protects private data. GLBA requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information. All electronic and paper data containing personally identifiable financial information must be protected. The penalty for noncompliance for a class of individuals is up to $500,000.
- *California's Database Security Breach Notification Act (2003)*. **California's Database Security Breach Notification Act** was the first state law that covers any state agency, person, or company that does business in California. It requires businesses to inform California residents within 48 hours if a breach of personal information has or is believed to have occurred. It defines personal information as a name with a Social Security number, driver's license number, state ID card, account number, credit card number, or debit card number and required security access codes. Since this act was passed by California in 2003, all other states now have similar laws with the exception of Alabama, Kentucky, New Mexico, and South Dakota.




Although these laws pertain to the United States, other nations are enacting their own legislation to protect electronic data.

The penalties for violating these laws can be sizable. Businesses must make every effort to keep electronic data secure from hostile outside forces to ensure compliance with these laws and avoid serious legal consequences.

**Maintaining Productivity** Cleaning up after an attack diverts resources such as time and money away from normal activities. Employees cannot be productive and complete important tasks during an attack and its aftermath because computers and networks cannot function properly. Table 1-6 provides a sample estimate of the lost wages and productivity during an attack and the subsequent cleanup.

| Number of total employees | Average hourly salary | Number of employees to combat attack | Hours required to stop attack and clean up | Total lost salaries | Total lost hours of productivity |
|---|---|---|---|---|---|
| 100 | $25 | 1 | 48 | $4,066 | 81 |
| 250 | $25 | 3 | 72 | $17,050 | 300 |
| 500 | $30 | 5 | 80 | $28,333 | 483 |
| 1,000 | $30 | 10 | 96 | $220,000 | 1,293 |

**Table 1-6** Cost of attacks


The single most expensive malicious attack was the Love Bug in 2000, which cost an estimated $8.7 billion.[21]

**Foiling Cyberterrorism** The FBI defines **cyberterrorism** as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Unlike an attack that is designed to steal information or erase a user's hard disk drive, cyberterrorism attacks are intended to cause panic, provoke violence, or result in a financial catastrophe.

The U.S. Commission of Critical Infrastructure Protection identifies possible cyberterrorist targets as the banking industry, military installations, power plants, air traffic control centers, and water systems. These are likely targets because they can significantly disrupt business and personal activities by destroying relatively few targets. For example, disabling an electrical power plant could cripple businesses, homes, transportation services, and communications over a wide area.


One of the challenges in combatting cyberterrorism is that many of the prime targets are not owned and managed by the federal government. For example, almost 85 percent of the nation's most critical computer networks and infrastructures are owned by private companies.[22] Because these networks are not centrally controlled, it is difficult to coordinate and maintain security.

# Who Are the Attackers?

The types of individuals behind computer attacks are generally divided into several categories. These include hackers, script kiddies, spies, insiders, cybercriminals, and cyberterrorists.

## Hackers

In the past, the term **hacker** was commonly used to refer to a person who uses advanced computer skills to attack computers. *White hat hackers* said that their goal was only to expose security flaws and not steal or corrupt data. Although breaking into another computer system is illegal, they considered it acceptable as long as they did not commit theft, vandalism, or breach any confidentiality while trying to improve security by seeking out vulnerabilities. In contrast, the term *black hat hackers* was used to refer to attackers whose motive was malicious and destructive.

However, today the term *hacker* has been replaced with the more generic term *attacker,* without any attempt to distinguish between the motives. Although "hacker" is often used by the mainstream media to refer to an attacker, this term is no longer commonly used by the security community.

## Script Kiddies

**Script kiddies** are individuals who want to break into computers to create damage yet lack the advanced knowledge of computers and networks needed to do so. Instead, script kiddies do their work by downloading automated attack software (*scripts*) from Web sites and using it to perform malicious acts.

Today, these scripts have been replaced by attack software with menu systems. This makes creating attacks even easier for these unskilled users. Figure 1-5 shows that over 40 percent of attacks are conducted by script kiddies with low or no skills.

## Spies

A computer **spy** is a person who has been hired to break into a computer and steal information. Spies do not randomly search for unsecured computers to attack as script kiddies and other attackers do; rather, spies are hired to attack a specific computer or system that contains sensitive information. Their goal is to break into that computer and take the information without drawing any attention to their actions. Spies generally possess excellent computer skills to attack and then cover their tracks.

## Insiders

Another serious threat to an organization actually comes from an unlikely source—its employees, contractors and business partners—often called *insiders*. In one study of 900 cases of business "data leakage," over 48 percent of the breaches were attributed to insiders who abused their right to access corporate information.[23]


In most instances, insider attacks are more costly than an attack from the outside.

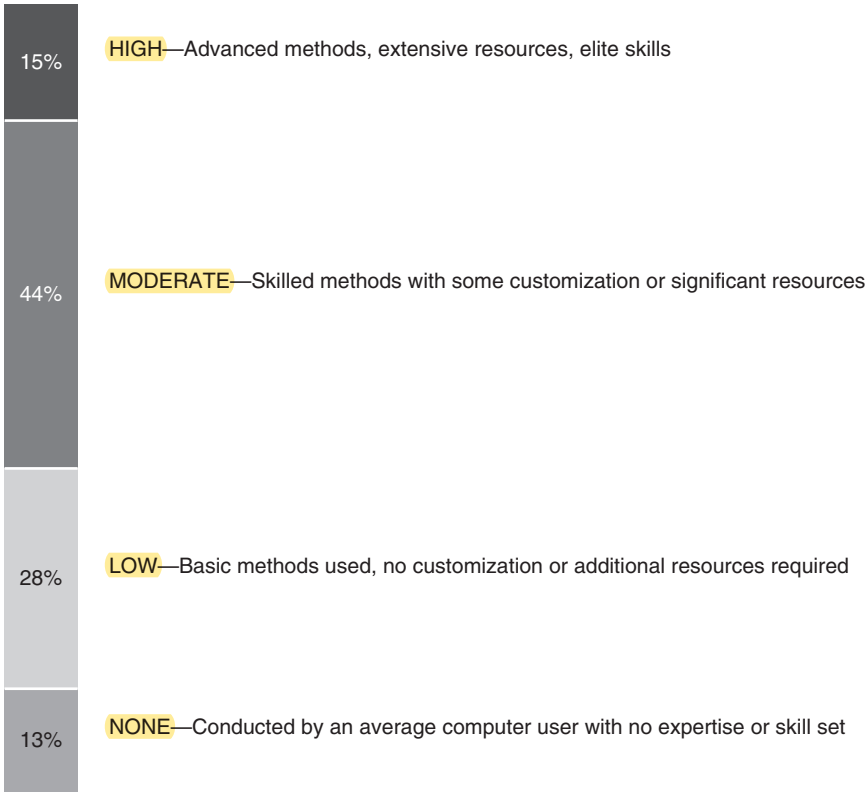



**Figure 1-5** Skills needed for creating attacks



Examples of several recent high-profile insider attacks include the following:

- A California health care worker, disgruntled over an upcoming job termination, illegally gathered health records on celebrities and distributed them to the media.
- A Maryland government employee tried to destroy the contents of over 4,000 servers by planting a malicious coding script that was scheduled to activate 90 days after he was terminated.
- A French securities trader lost over $7 billion on bad stock bets and then used his knowledge of the bank's computer security system to conceal the losses through fake transactions.
- A U.S. Army private in Iraq accessed secret U.S. diplomatic cables and other sensitive documents, which were then given to an international whistleblower who posted them on the Internet.

Most insider attacks are either the sabotage or theft of intellectual property. One study revealed that most cases of sabotage come from employees who have announced their resignation or who have been formally reprimanded, demoted, or fired. When theft is involved, the offenders are usually salespeople, engineers, computer programmers, or scientists who actually believe that the accumulated data is owned by them and not the organization (most of these thefts occur within 30 days of the employee resigning). In some instances, the employees are moving to a new job and want to take "their work" with them, while in other cases the employees have been bribed

or pressured into stealing the data. In about 8 percent of the incidences of theft, employees have been pressured into stealing from their employer through blackmail or threat of violence.[24]


Although it generally is not intentional, in many instances, carelessness by employees has resulted in serious security breaches. For example, almost 10,000 laptop computers each week are lost in airports, and over half contain confidential or sensitive information. Only one out of every three lost laptops is returned to their owner. The two U.S. airports reporting the highest number of missing laptops are Los Angeles International and Miami International airports.[25]

## Cybercriminals

There is a new breed of computer attackers known as **cybercriminals**. Cybercriminals are a network of attackers, identity thieves, spammers, and financial fraudsters. These cybercriminals are described as being more highly motivated, less risk-averse, better funded, and more tenacious than ordinary attackers.

Some security experts believe that many cybercriminals belong to organized gangs of young attackers, often clustered in Eastern European, Asian, and third-world regions. Reasons these areas may harbor large number of cybercriminals are summarized in Table 1-7.

| Characteristic | Explanation |
|---|---|
| Strong technical universities | Since the demise of the Soviet Union in the early 1990s, a number of large universities have stopped teaching communist ideology and turned to teaching technology |
| Low incomes | With the transition from communism to a free market system, individuals in several nations have suffered from the loss of an economy supported by the state, and incomes remain relatively low |
| Unstable legal systems | Many nations continue to struggle with making and enforcing new laws that combat computer crime |
| Tense political relations | Some new nations do not yet have strong ties to other foreign countries, and this sometimes complicates efforts to obtain cooperation with local law enforcement |

**Table 1-7** Characteristics of cybercriminals


Cybercriminals often meet in online "underground" forums that have names like *DarkMarket.org* and *theftservices.com*. The purpose of these meetings is to trade information and coordinate attacks around the world.

Instead of attacking a computer to show off their technology skills (*fame*), cybercriminals have a more focused goal of financial gain (*fortune*). Cybercrimminals use vulnerabilities to steal information or launch attacks that can generate income. This difference makes the new attackers more dangerous and their attacks more threatening. These targeted attacks against financial networks, unauthorized access to information, and the theft of personal information are sometimes known as **cybercrime**.

Financial cybercrime is often divided into two categories. The first uses stolen data, credit card numbers, online financial account information, or Social Security numbers to steal from its victims. The second category involves sending millions of spam e-mails to peddle counterfeit drugs, pirated software, fake watches, and pornography. Federal law enforcement officials estimate that these spam operations gross hundreds of millions of dollars annually. One security professional estimates that the cybercrime industry netted $1 *trillion* in 2010.[26]


Some security experts maintain that European cybercriminals are mostly focused on activities to steal money from their victims, while cybercriminals from Asia are more interested in stealing data from governments or corporations.

### Cyberterrorists

Many security experts fear that terrorists will turn their attacks to a nation's network and computer infrastructure to cause panic among citizens. Known as **cyberterrorists**, their motivation may be defined as ideology, or attacking for the sake of their principles or beliefs. A report distributed by the Institute for Security Technology Studies at Dartmouth College lists three goals of a cyberattack:

- To deface electronic information (such as Web sites) and spread misinformation and propaganda
- To deny service to legitimate computer users
- To commit unauthorized intrusions into systems and networks that result in critical infrastructure outages and corruption of vital data

Cyberterrorists are sometimes considered the attackers that should be feared the most, for it is almost impossible to predict when or where an attack may occur. Unlike cybercriminals who continuously probe systems or create attacks, cyberterrorists can be inactive for several years and then suddenly strike in a new way. Their targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

## Attacks and Defenses

Although a wide variety of attacks can be launched against a computer or network, the same basic steps are used in most attacks. Protecting computers against these steps in an attack calls for following five fundamental security principles.

### Steps of an Attack

There are a variety of types of attacks. One way to categorize these attacks is by the five steps that make up an attack, as seen in Figure 1-6. The steps are:

1. *Probe for information.* The first step in an attack is to probe the system for any information that can be used to attack it. This type of "reconnaissance" is essential to provide information, such as the type of hardware used, version of software or firmware, and even personal information about the users, that can then be used in the

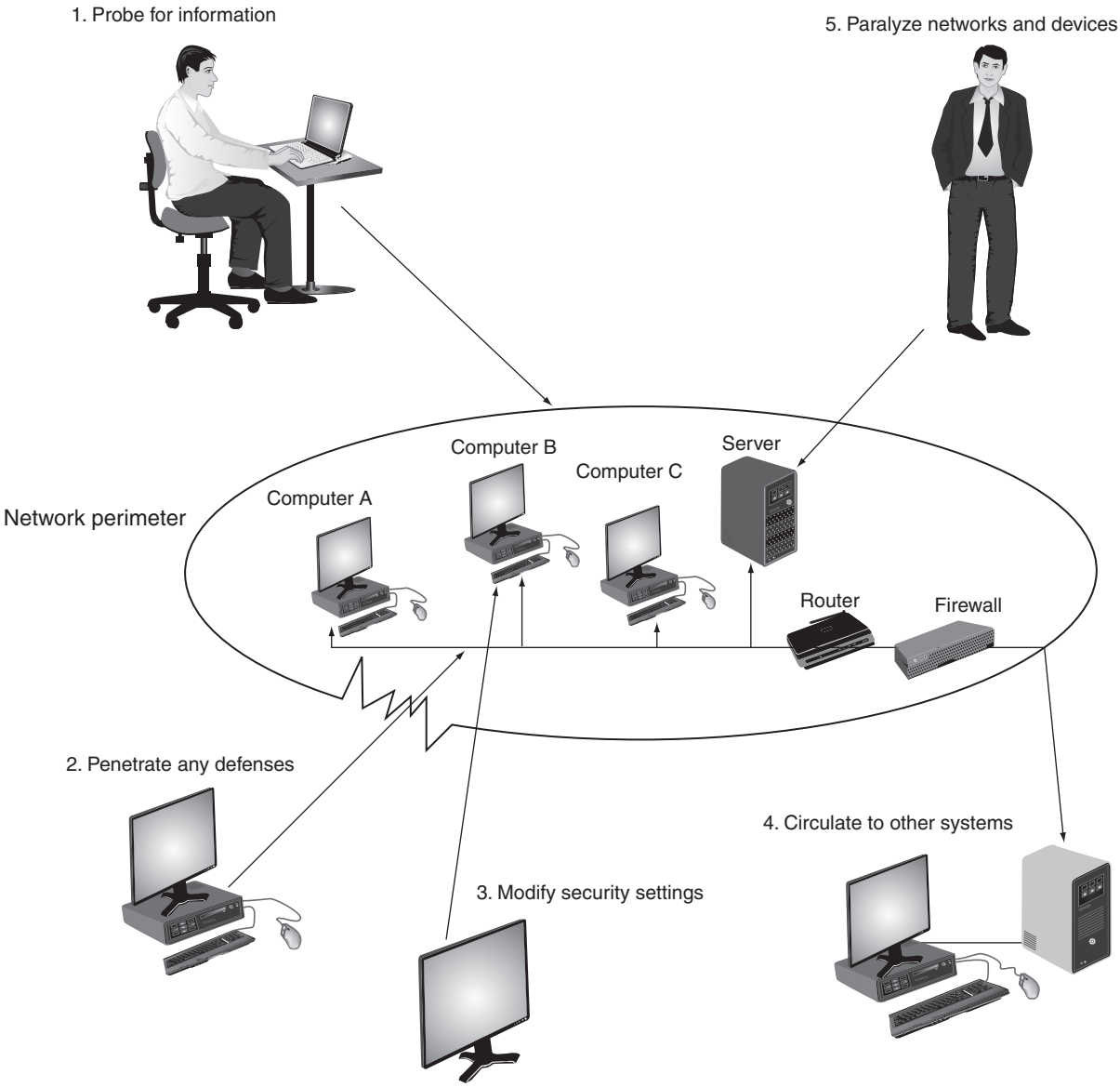



**Figure 1-6** Steps of an attack





next step. Actions that take place in probing for information include "ping sweeps" of the network to determine if a system responds, port scanning for determining which ports may be accessible, and queries that respond with failure messages yet provide valuable information about the system.

2. *Penetrate any defenses*. Once a potential system has been identified and information about it has been gathered, the next step is to launch the attack to penetrate the defenses. These attacks come in a variety of forms.

3. *Modify security settings*. Modifying the security settings is the next step after the system has been penetrated. This allows the attacker to reenter the compromised system more easily.
4. *Circulate to other systems*. Once the network or system has been compromised, the attacker then uses it as a base of attack toward other networks and computers. The same tools that are used to probe for information are then directed toward other systems.
5. *Paralyze networks and devices*. If the attacker chooses, she may also work to maliciously damage the infected computer or network. This may include deleting or modifying critical operating system files or injecting software that will prevent the computer from properly functioning.

## Defenses Against Attacks

Although multiple defenses may be necessary to withstand an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity. These principles provide a foundation for building a secure system.

### Layering

The Crown Jewels of England, which are worn during coronations and important state functions, have a dollar value of over $32 million, yet are virtually priceless as symbols of English culture. How are precious stones like the Crown Jewels protected from theft? They are not openly displayed on a table for anyone to pick up. Instead, they are enclosed in protective cases with two-inch-thick glass that is bulletproof, smashproof, and resistant to almost any outside force. The cases are located in a special room with massive walls and sensors that can detect slight movements or vibrations. The doors to the room are monitored around the clock by remote security cameras, and the video images from each camera are recorded. The room itself is in the Tower of London, surrounded by roaming guards and fences. In short, these precious stones are protected by *layers* of security. If one layer is penetrated—such as the thief getting into the building—several more layers must still be breached, and each layer is often more difficult or complicated than the previous. A layered approach has the advantage of creating a barrier of multiple defenses that can be coordinated to thwart a variety of attacks.

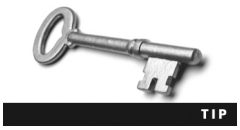

The Jewel House, which holds the Crown Jewels in the Tower of London, is actually located inside an Army barracks that is staffed with soldiers.

Likewise, information security must be created in layers. If only one defense mechanism is in place, an attacker only has to circumvent that single defense. Instead, a security system must have layers, making it unlikely that an attacker has the tools and skills to break through *all* the layers of defenses. A layered approach can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

## Limiting

Consider again protecting the Crown Jewels of England. Although the jewels may be on display for the general public to view, permitting anyone to touch them increases the chances that they will be stolen. Only approved personnel should be authorized to handle the jewels. Limiting who can access the jewels reduces the threat against them.

The same is true with information security. Limiting access to information reduces the threat against it. This means that only those personnel who must use the data should have access to it. In addition, the type of access they have should also be limited to what that person needs to perform their job. For example, access to the human resource database for an organization should be limited to only employees who have a genuine need to access it, such as human resource personnel or vice presidents. And, the type of access should also be restricted: human resource employees may be able to view employee salaries but not change them.




What level of access should users have? The best answer is the *least amount necessary* to do their jobs, and no more.

Some ways to limit access are technology-based (such as assigning file permissions so that a user can only read but not modify a file), while others are procedural (prohibiting an employee from removing a sensitive document from the premises). The key is that access must be restricted to the bare minimum.

## Diversity

Diversity is closely related to layering. Just as it is important to protect data with layers of security, the layers must also be different (diverse). This means that if attackers penetrate one layer, they cannot use the *same* techniques to break through all other layers. A jewel thief, for instance, might be able to foil the security camera by dressing in black clothing, but should not be able to use the same technique to trick the motion detection system. Using diverse layers of defense means that breaching one security layer does not compromise the whole system.

Information security diversity may be achieved in several ways. For example, some organizations use security products provided by different manufacturers. An attacker who can circumvent a security device from Manufacturer A could then use those same skills and knowledge to defeat all of the same devices used by the organization. However, if devices from Manufacturer A and similar devices from Manufacturer B were both used by the same organization, the attacker would have more difficulty trying to break through both types of devices because they are different.

## Obscurity

Suppose a thief plans to steal the Crown Jewels during a shift change of the security guards. When the thief observes the guards, however, she finds that the guards do not change shifts at the same time each night. On a given Monday, they rotate shifts at 2:13 AM, while on Tuesday they rotate at 1:51 AM, and the following Monday at 2:24 AM. Because the shift changes cannot be known for certain in advance, the planned attack cannot be carried out. This technique is sometimes called *security by obscurity*: obscuring to the outside world what is on the inside makes attacks that much more difficult.

An example of obscurity in information security would be not revealing the type of computer, version of operating system, or brand of software that is used. An attacker who knows that information could use it to determine the vulnerabilities of the system to attack it. However, if this information is concealed, it is more difficult to attack a system when nothing is known about it and is hidden from the outside. Obscuring information can be an important means of protection.

### Simplicity

Because attacks can come from a variety of sources and in many ways, information security is by its very nature complex. Yet the more complex it becomes, the more difficult it is to understand. A security guard who does not understand how motion detectors interact with infrared trip lights may not know what to do when one system alarm shows an intruder but the other does not. In addition, complex systems allow many opportunities for something to go wrong. In short, complex systems can be a thief's ally.

The same is true with information security. Complex security systems can be hard to understand, troubleshoot, and even feel secure about. As much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with, yet this can also make it easier for the attackers. In short, keeping a system simple from the inside, but complex on the outside, can sometimes be difficult but reaps a major benefit.

## Chapter Summary

- Attacks against information security have grown exponentially in recent years, despite the fact that billions of dollars are spent annually on security. No computer system is immune from attacks or can be considered entirely secure.
- There are several reasons it is difficult to defend against today's attacks. These reasons include the fact that virtually all devices are connected to the Internet, the speed of the attacks, greater sophistication of attacks, the availability and simplicity of attack tools, faster detection of vulnerabilities by attackers, delays in patching, weak patch distribution, distributed attacks coming from multiple sources, and user confusion.
- Information security may be defined as that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures. As with many advanced subjects, information security has its own set of terminology. A threat is an event or action that represents a danger to information assets, which is something that has value. A threat agent is a person or element that has the power to carry out a threat, usually by exploiting a vulnerability, which is a flaw or weakness. A risk is the likelihood that a threat agent will exploit the vulnerability.
- The main goals of information security are to prevent data theft, thwart identify theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.
- The types of people behind computer attacks fall into several categories. The term hacker generally refers to someone who attacks computers. Script kiddies do their work by downloading automated attack software from Web sites and then using it to

break into computers. A computer spy is a person who has been hired to break into a computer and steal information. One of the largest information security threats to a business actually comes from its employees. A new breed of computer attackers is known as cybercriminals, who are a loose-knit network of attackers, identity thieves, and financial fraudsters. Cyberterrorists are motivated by their principles and beliefs, and turn their attacks to the network and computer infrastructure to cause panic among citizens.

- There are a variety of types of attacks. Five general steps make up an attack: probe for information, penetrate any defenses, modify security settings, circulate to other systems, and paralyze networks and devices. Although multiple defenses may be necessary to withstand the steps of an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity.

## Key Terms

**accounting** The ability that provides tracking of events.

**asset** An item that has value.

**authorization** The act of ensuring that an individual or element is genuine.

**authentication** The steps that ensure that the individual is who they claim to be.

**availability** Security actions that ensure that data is accessible to authorized users.

**California's Database Security Breach Notification Act** The first state law that covers any state agency, person, or company that does business in California.

**confidentiality** Security actions that ensure only authorized parties can view the information.

**cybercrime** Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information.

**cybercriminals** A network of attackers, identity thieves, spammers, and financial fraudsters.

**cyberterrorism** A premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence.

**cyberterrorists** Attackers whose motivation may be defined as ideology, or attacking for the sake of their principles or beliefs.

**exploiting** The act of taking advantage of a vulnerability.

**Gramm-Leach-Bliley Act (GLBA)** A law that requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information.

**hacker** A term used to refer to a person who uses advanced computer skills to attack computers.

**Health Insurance Portability and Accountability Act (HIPAA)** A law designed to guard protected health information and implement policies and procedures to safeguard it.

**identity theft** Stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain.