Securing Information Systems

CHAPTER 7

STUDENT LEARNING OBJECTIVES

After completing this chapter, you will be able to answer the following questions:

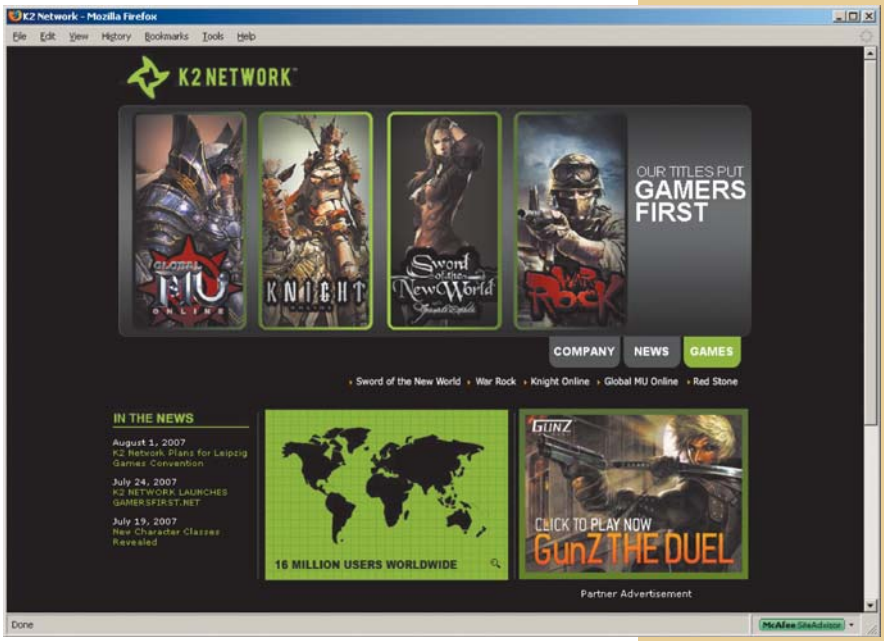
1. Why are information systems vulnerable to destruction, error, and abuse?
2. What is the business value of security and control?
3. What are the components of an organizational framework for security and control?
4. What are the most important tools and technologies for safeguarding information resources?

Chapter Outline

ONLINE GAMES NEED SECURITY, TOO

Have you ever played War Rock, Knight Online, or Sword of the New World? They are all massively multiplayer online games from K2 Network, which is based in Irvine, California. K2 currently has about 16 million registered users around the world. Its motto is "Gamers First," and it is known for its compelling titles, creative pricing, quality customer service, and frequent updates based on user requests.

If you have played any of these games, you have some idea of how much K2 puts into "Gamers First"—fantastic clothing and armor sets, fast-paced action, and the ability to control multiple characters at the same time, each with multiple stances and skills. Players are allowed to enter a game for free, but must buy digital "assets" from K2, such as swords to fight dragons, if they want to be deeply involved. The games can accomodate millions of players at once and are played simultaneously by people all over the world. What you may not see is how much K2 puts into protecting its Web sites from hacker attacks.



K2 would lose a great deal of money if its game sites were not working, as well as damage its brand reputation. It does not want hackers attacking its Web sites to extort money from players, to steal their gaming assets, or to steal customer information.

When K2 launched its first game in North America in 2003, it was using Secure Sockets Layer (SSL) certificates to encrypt communications with players buying its gaming assets. This did not offer enough protection against hackers who knew how to exploit flaws in Web applications, such as being able to enter commands into a Web browser that fools a database into revealing its contents. So K2 turned to two other security products—NetContinuum's NC-2000 AG firewall and Cenzic's ClickToSecure managed service. Using these tools in concert, K2 is able to detect flaws in its software, make sure those flaws are not reintroduced when new software is being developed, and protect its software against attacks. Cenzic's service remotely probes K2's applications as a hacker would and reports any vulnerabilities it finds, along with suggestions for eliminating them. Cenzic continually monitors hacker activity and upgrades its products to deal with new vulnerabilities and hacker techniques. NetContinuum's firewall is a box that sits in front of a Web server to examine network traffic and block suspicious traffic.

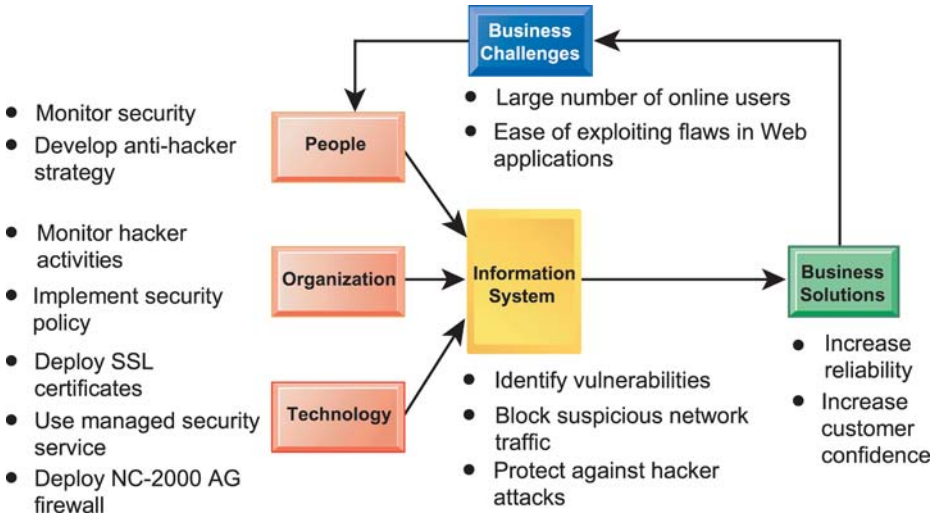
K2 spent nearly $250,000 on security in 2006 and expects to spend a similar amount in 2007. Management believes the money is well spent. K2's Web sites have never been breached.

Sources: Deborah Gage, "Stop Playing with Hackers," *Baseline*, February 2007 and www.k2network.com, accessed July 17, 2007.

The problems created by hackers for K2 Network and online game players illustrate some of the reasons why businesses need to pay special attention to information system security. Web sites such as those of K2 Network are vulnerable to malicious attacks designed to disable them and prevent their businesses from operating. If K2's game sites were not operational for even a day, the company would lose many millions of dollars, and possibly the loyalty of its subscribers.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. K2's sites attract millions of people, making them attractive targets for hackers. The open nature of Internet connections makes Web applications vulnerable. Web software developers charged with getting new products to market quickly may not have detected all the vulnerabilities and errors.

K2 could have continued to rely on Secure Sockets Layer (SSL) encryption to secure communication with its players. But management realized this was not enough, and that the stakes were too high to allow hackers to exploit flaws in its Web applications. The company decided to make heavy investments in security technology to provide added layers of protection. It installed a firewall to filter out suspicious network traffic, and it subscribed to a service that monitors hacker activity, continually probes K2's software applications to detect vulnerabilities, and provides recommendations for eliminating them. The chosen solution has kept K2's game sites secure.



HEADS UP

This chapter focuses on how to secure your information systems and the information inside them. As e-commerce and e-business have grown to encompass so much of our lives, we have all become much more aware of the need to secure digital information. Your customers expect you to keep their digital private information secure and confidential. As your business increasingly relies on the Internet, you will become vulnerable to a variety of attacks against your systems that could, if successful, put you out of business in a very short time. To protect your business, you will need to pay more attention to security and control than ever before.

7.1 System Vulnerability and Abuse

Can you imagine what would happen if you tried to link to the Internet without a firewall or antivirus software? Your computer would be disabled in a few seconds, and it might take you many days to recover. If you used the computer to run your business, you might not be able to sell to your customers or place orders with your suppliers while it was down. And you might find that your computer system had been penetrated by outsiders, who perhaps stole or destroyed valuable data, including confidential payment data from your customers. If too much data were destroyed or divulged, your business might never be able to operate!

In short, if you operate a business today, you need to make security and control a top priority. **Security** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. **Controls** are methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its records, and operational adherence to management standards.

WHY SYSTEMS ARE VULNERABLE

When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they existed in manual form. Through communications networks,

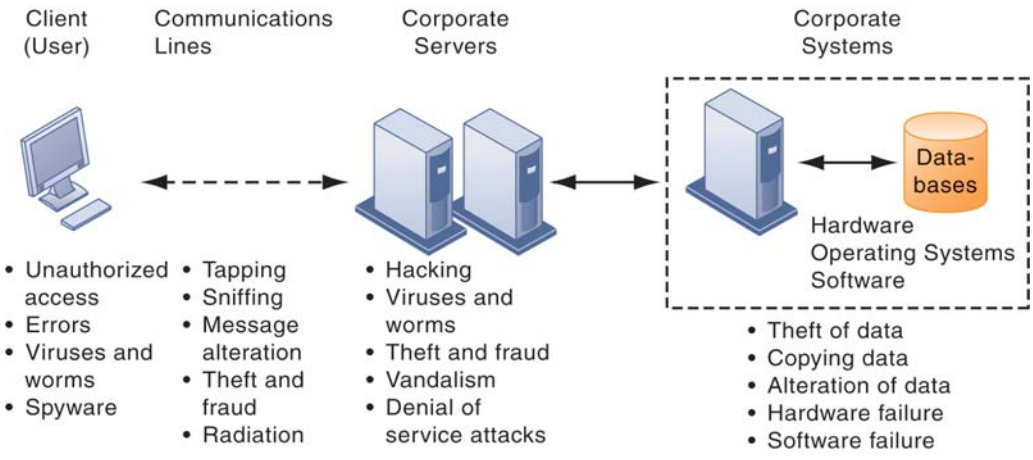


Figure 7-1 Contemporary Security Challenges and Vulnerabilities
The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

information systems in different locations are interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network.

Figure 7-1 illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multi-tier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-of-service attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can destroy or alter corporate data stored in databases or files.

Systems malfunction if computer hardware breaks down, is not configured properly, or is damaged by improper use or criminal acts. Errors in programming, improper installation, or unauthorized changes cause computer software to fail. Power failures, floods, fires, or other natural disasters can also disrupt computer systems.

Domestic or offshore partnering with another company adds to system vulnerability if valuable information resides on networks and computers outside the organization's control. Without strong safeguards, valuable data could be lost, destroyed, or could fall into the wrong hands, revealing important trade secrets or information that violates personal privacy.

Internet Vulnerabilities

Large public networks, such as the Internet, are more vulnerable than internal networks because they are virtually open to anyone. The Internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.

Computers that are constantly connected to the Internet, such as those that connect by cable modems or digital subscriber line (DSL) modems, are more open to penetration by outsiders because they use fixed Internet addresses for long periods, so they can be easily identified. (With dial-up service, a temporary Internet address is assigned for each session.) A fixed Internet address creates a fixed target for hackers.

Telephone service based on Internet technology (see Chapter 6) is more vulnerable than the switched voice network if it does not run over a secure private network. Most Voice over IP (VoIP) traffic over the public Internet is not encrypted, so anyone with a network can listen in on conversations. Hackers can intercept conversations or shut down voice service by flooding servers supporting VoIP with bogus traffic.

Vulnerability has also increased from widespread use of e-mail and instant messaging (IM). E-mail may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients. Popular IM applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by outsiders during transmission over the public Internet. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network.

Wireless Security Challenges

Is it safe to log onto a wireless network at an airport, library, or other public location? It depends on how vigilant you are. Even the wireless network in your home is vulnerable because radio frequency bands are easy to scan. Both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers.

Although the range of wireless fidelity (Wi-Fi) networks is only several hundred feet, it can be extended up to one-fourth of a mile using external antennae. Local area networks (LANs) using the 802.11 standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic, and, in some cases, gain access to the Internet or to corporate networks. The chapter-ending case describes how poor wireless security may have enabled hackers to break into TJX Companies' corporate systems and steal credit card and personal data on nearly 46 million people.

Wi-Fi transmission technology was designed to make it easy for stations to find and hear one another. The *service set identifiers (SSIDs)* identifying the access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by intruders' sniffer programs (see Figure 7-2). Wireless networks in many locations do not have basic protections against **war driving**, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

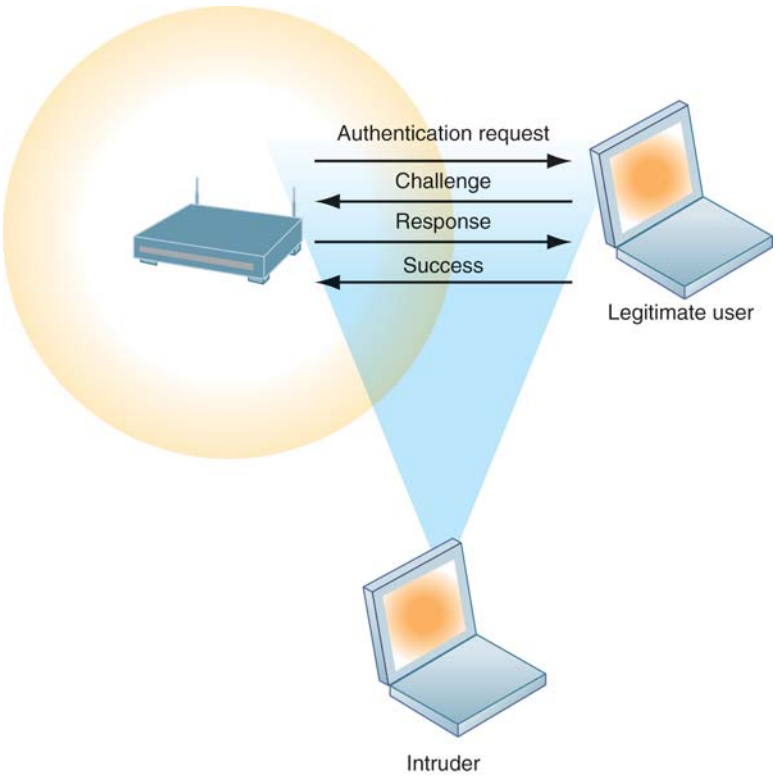


Figure 7-2
Wi-Fi Security Challenges
Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

A hacker can employ an 802.11 analysis tool to identify the SSID. (Windows XP has capabilities for detecting the SSID used in a network and automatically configuring the radio NIC within the user's device.) An intruder that has associated with an access point by using the correct SSID is capable of accessing other resources on the network, using the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files.

Intruders also use the information they have gleaned to set up rogue access points on a different radio channel in physical locations close to users to force a user's radio NIC to associate with the rogue access point. Once this association occurs, hackers using the rogue access point can capture the names and passwords of unsuspecting users.

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective. WEP is built into all standard 802.11 products, but its use is optional. Many users neglect to use WEP security features, leaving them unprotected. The basic WEP specification calls for an access point and all of its users to share the same 40-bit encrypted password, which can be easily decrypted by hackers from a small amount of traffic. Stronger encryption and authentication systems are now available, but users must be willing to install them.

MALICIOUS SOFTWARE: VIRUSES, WORMS, TROJAN HORSES, AND SPYWARE

Malicious software programs are referred to as **malware** and include a variety of threats, such as computer viruses, worms, and Trojan horses. A **computer virus** is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission. Most computer viruses deliver a "payload." The payload may be relatively benign, such as the instructions to display a message or image, or it may be highly destructive—destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly. Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file.

Most recent attacks have come from **worms**, which are independent computer programs that copy themselves from one computer to other computers over a network. (Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer. This explains why computer worms spread much more rapidly than computer viruses.) Worms destroy data and programs as well as disrupt or even halt the operation of computer networks.

Worms and viruses are often spread over the Internet from files of downloaded software, from files attached to e-mail transmissions, or from compromised e-mail messages or instant messaging. Viruses have also invaded computerized information systems from "infected" disks or infected machines. E-mail worms are currently the most problematic.

In 2006, antivirus vendors detected more than 200 viruses and worms targeting mobile phones, such as CABIR, Comwarrior, and Frontal A (Gaur and Kiep, 2007). Frontal A, for example, installs a corrupted file that causes phone failure and prevents the user from rebooting. Mobile device viruses could pose serious threats to enterprise computing because so many wireless devices are now linked to corporate information systems.

Web 2.0 applications, such as blogs, wikis, and social networking sites such as MySpace, have emerged as new conduits for malware or spyware. These applications allow users to post software code as part of the permissible content, and such code can be launched automatically as soon as a Web page is viewed. For example, in November 2006, Wikipedia was compromised and used to distribute malware among unsuspecting users who thought they were obtaining information about a security patch (Secure Computing, 2007).

Table 7.1 describes the characteristics of some of the most harmful worms and viruses that have appeared to date.

Over the past decade, worms and viruses have cause billions of dollars of damage to corporate networks, e-mail systems, and data. According to Consumer Reports' State of the

TABLE 7.1

Examples of Malicious Code

Name	Type	Description
Netsky.P	Worm/ Trojan horse	First appeared in early 2003 and was still one of the most common computer worms in 2007. Spreads by gathering target e-mail addresses from the computers it infects, and sending e-mail to all recipients from the infected computer. Commonly used by bot networks to launch spam and denial-of-service attacks.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot, and infected computers to search for more victims. Affected millions of computers worldwide, disrupting British Airways flight check-ins, operations of British coast guard stations, Hong Kong hospitals, Taiwan post office branches, and Australia's Westpac Bank. Sasser and its variants caused an estimated $14.8 billion to $18.6 billion in damages worldwide.
MyDoom.A	Worm	First appeared January 26, 2004. Spreads as an e-mail attachment. Sends e-mail to addresses harvested from infected machines, forging the sender's address. At its peak, this worm lowered global Internet performance by 10 percent and Web page loading times by as much as 50 percent. Was programmed to stop spreading after February 12, 2004.
Bagle	Worm	First appeared January 18, 2004. Infected PCs via an e-mail attachment, then used the PC e-mail addresses for replicating itself. Infected PCs and their data could be accessed by remote users and applications. Bagle.B stopped spreading after January 28, 2004, but other variants are still active. Has caused tens of millions of dollars in damage already.
Sobig.F	Worm	First detected on August 19, 2003. Spreads via e-mail attachments and sends massive amounts of mail with forged sender information. Deactivated itself on September 10, 2003, after infecting more than 1 million PCs and doing $5 to $10 billion in damage.
ILoveYou	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.
Melissa	Macro virus/worm	First appeared in March 1999. Word macro script mailing infected Word file to first 50 entries in user's Microsoft Outlook address book. Infected 15 to 29 percent of all business PCs, causing $300 million to $600 million in damage.

Internet survey, U.S. consumers lost $7.9 billion because of malware and online scams, and the majority of these losses came from malware (Software World, 2006).

A **Trojan horse** is a software program that appears to be benign but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate but is often a way for viruses or other malicious code to be introduced into a computer system. The term *Trojan horse* is based on the huge wooden horse used by the Greeks to trick the Trojans into opening the gates to their fortified city during the Trojan War. Once inside the city walls, Greek soldiers hidden in the horse revealed themselves and captured the city.

An example of a modern-day Trojan horse is BotVoice.A, detected in July 2007. Once this Trojan horse is installed, it deletes everything from the victim's computer hard drive while repeating an audible message, "You have been infected." BotVoice.A infects computers running Windows operating systems and spreads via peer-to-peer file-sharing networks, CD-ROMs, or USB flash memory drives.

Some types of **spyware** also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising. Thousands of forms of spyware have been documented. Harris Interactive found that 92 percent of the companies surveyed in its Web@Work study reported detecting spyware on their networks (Mitchell, 2006).

Many users find such spyware annoying and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious. **Key loggers** record every keystroke made on a computer to steal serial numbers for software, launch Internet attacks, gain access to e-mail accounts, obtain passwords to protected computer systems, or pick up personal information such as credit card numbers. Other spyware programs reset Web browser home pages, redirect search requests, or slow computer performance by taking up too much memory.

HACKERS AND COMPUTER CRIME

A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term *cracker* is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use.

Hacker activities have broadened beyond mere system intrusion to include theft of goods and information, as well as system damage and **cybervandalism**, the intentional disruption, defacement, or even destruction of a Web site or corporate information system. For example, on August 20, 2006, Pakistani hackers broke into the computer hosting the Web site of Kevin Mitnick, an ex-hacker turned security consultant, and replaced the home page with one displaying a vulgar message (Evers, 2006).

Spoofing and Sniffing

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else. **Spoofing** also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site. We provide more detail on other forms of spoofing in our discussion of computer crime.

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers help identify potential network trouble spots or criminal activity on networks, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

Denial-of-Service Attacks

In a **denial-of-service (DoS) attack**, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A **distributed denial-of-service (DDoS)** attack uses numerous computers to inundate and overwhelm the network from numerous launch points. For example, Bill O'Reilly's official Web site was bombarded by data that overloaded the system's firewalls for two days in early March 2007, forcing the site to be taken down to protect it (Schmidt, 2007).

Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a Web site to shut down, making it impossible for legitimate users to access the site. For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. Especially vulnerable are small and midsize businesses whose networks tend to be less protected than those of large corporations.

Perpetrators of DoS attacks often use thousands of "zombie" PCs infected with malicious software without their owners' knowledge and organized into a **botnet**. Hackers create these botnets by infecting other people's computers with bot malware that opens a back door through which an attacker can give instructions. The infected computer then becomes a slave, or zombie, serving a master computer belonging to someone else. Once a hacker infects enough computers, her or she can use the amassed resources of the botnet to launch distributed denial-of-service attacks, phishing campaigns, or unsolicited "spam" e-mail.

In the first six months of 2007, security product provider Symantec observed over 5 million distinct bot-infected computers. Arguably, bots and bot networks are currently the single most important threat to the Internet and e-commerce because they can be used to launch very large scale attacks using many different techniques (Symantec, 2007). For example, the Storm worm, which was responsible for one of the largest e-mail attacks in the past few years, was propagated via a massive botnet of nearly 2 million computers (Gaudin, 2007). The Interactive Session on Technology provides more detail on the scope and severity of bot attacks.

Computer Crime

Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of computer crime as well. For example, Yung-Sun Lin was charged in January 2007 with installing a "logic bomb" program on the computers of his employer, Medco Health Solutions of Franklin Lakes, New Jersey. Lin's program could have erased critical prescription information for 60 million Americans (Gaudin, 2007). **Computer crime** is defined by the U.S. Department of Justice as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." Table 7.2 provides examples of the computer as a target of crime and as an instrument of crime.

No one knows the magnitude of the computer crime problem—how many systems are invaded, how many people engage in the practice, or the total economic damage. According to one study by the Computer Crime Research Center, U.S. companies lose approximately $14 billion annually to cybercrimes. Many companies are reluctant to report computer crimes because the crimes may involve employees or the company fears that publicizing its vulnerability will hurt its reputation. The most economically damaging kinds of computer crime are DoS attacks, introducing viruses, theft of services, and disruption of computer systems.

Identity Theft

With the growth of the Internet and electronic commerce, identity theft has become especially troubling. **Identity theft** is a crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials. According to Javelin Strategy & Research, 8.4 million Americans were victims of identity theft in 2006, and they suffered losses totaling $49.3 billion (Stempel, 2007).

INTERACTIVE SESSION: TECHNOLOGY — Bot Armies Launch a Digital Data Siege

In Estonia, the Internet is almost as vital as running water. People use it routinely to vote, to file their taxes, and to shop or pay for parking with their cell phones. When the Estonian government began removing a bronze Soviet-era war memorial statue from a Tallinn park in April 2007, the move incited rioting by ethnic Russians. But the most violent protests took place over the Internet.

Major Estonian Web sites were subject to a massive and sustained distributed-denial-of-service attack that crippled the Web sites of Estonia's president, prime minister, Parliament, government agencies, national bank, and several daily newspapers. The attackers used a giant network of bots—as many as 1 million computers in Russia, Estonia, and other countries, including the United States, Canada, Brazil and Vietnam. They even rented time on other botnets. The attacks started around April 26 and lasted for nearly a month. The 10 largest assaults blasted streams of 90 megabits of data per second at Estonia's networks, lasting up to 10 hours each. This data load is equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours.

Estonia's Computer Emergency Response team gathered security experts from Estonian Internet service providers, banks, government agencies, and authorities in other countries to help track down and block traffic from suspicious Internet addresses. Estonia had to close off large parts of its network to people outside the country and focused on trying to protect the most essential sites, including online banking. On May 10, the attackers' time on rented servers expired, and the botnet attacks fell off abruptly. The last major wave of attacks occurred on May 18.

Because it is so easy for attackers to conceal their Internet addresses and harness other computers to do their work, experts believe that the attackers would probably never be caught. They also believe that attacks such as these will become even more severe in the coming years, as bots are harnessed for more acts of cyberwarfare and other illicit activities.

Building and selling bots for malicious purposes has become a serious money-making enterprise. James Ancheta, a self-taught computer expert, pleaded guilty on January 23, 2006, in the U.S. District Court in Los Angeles to building and selling bots and using his network of thousands of bots to commit crimes. His botnet infected at least 400,000 computers, including machines at two U.S. Department of Defense facilities, and had installed unauthorized adware that earned him more than $60,000.

Ancheta also rented or sold bots to people interested in using them to send spam or launch DoS attacks to disable specific Web sites. Ancheta's botz4sale Web site offered access to up to 10,000 compromised PCs at one time for as little as 4 cents each.

To outwit law enforcement, Ancheta continually changed e-mail addresses, ISPs, domain names, and instant messaging handles. Eventually his luck ran out. The FBI arrested him on November 3, 2005, and shut down his operations. Ancheta was sentenced to 57 months in federal prison.

Could bot attacks like these be prevented? It's getting increasingly difficult. According to Michael Lines, chief security officer at credit reporting firm TransUnion, "There is no single technology or strategy to [solve] the problem." Even if people use antivirus and antispyware software and patch software vulnerabilities, new bots appear that target different vulnerabilities.

Hackers don't even have to write their own bot programs. They can download bot toolkits for free on the Internet. Ancheta modified Rxbot, a bot strain available for download at several Web sites, and had his bots report to an Internet Relay Chat (IRC) channel that he controlled. And as the Ancheta case revealed, people can even buy access to bots.

How do you know if your computers are being used in botnets? Warning signs include systems that seem to be running too slowly, have unusual spikes in network traffic, or get too many pop-up ads.

What can you do about it? At the very least, regularly patch software and keep firewalls and antivirus software up to date, including antivirus and filtering software for instant messaging. Companies should also use tools to monitor not only inbound network traffic for malware and suspicious behavior but also outbound traffic leaving the network, in the event this traffic contains malware from an infected computer that could be used to recruit additional bots.

The most common approach today when your network is being attacked by a botnet is to cut off all traffic to any servers that are being targeted, as the Estonian government did. This, however, isn't a way to solve the problem as much as it is a way to address immediate concerns. What is more effective, and more difficult, is to have cooperation among botnet victims, ISPs, and law enforcement worldwide. Trend Micro, a leading provide of antivirus software and online security tools, offers a free anti-botnet service that will notify users if their machine

has been hijacked by a botnet or if information from their machine is being stolen and transmitted to the bot master.

Sources: Mark Landler and John Markoff, "War Fears Turn Digital After Data Siege in Estonia," *The New York Times*, May 29, 2007; Joaquim P. Menezs, "The Botnet Menace-and What You Can Do About It, "IT World Canada, June 4, 2007; Deborah Gage, "Security Case: How to Survive a Bot Attack," *Baseline*, February 6, 2007; Deborah Gage and Kim S. Nash, "When Bots Attack," *Baseline*, April 2006; and Robert Lemos, "Major Prison Time for Bot Master," *Security Focus*, May 9, 2006.

CASE STUDY QUESTIONS

1. What is the business impact of botnets?
2. What people, organization, and technology factors should be addressed in a plan to prevent botnet attacks?
3. How easy would it be for a small business to combat botnet attacks? A large business?
4. How would you know if your computer was part of a botnet? Explain your answer.

MIS IN ACTION

Read the article on "Robot Wars-How Botnets Work" by Massimiliano Romano, Simone Rosignoli, and Ennio Giannini at WindowsSecurity.com. Prepare an electronic presentation that summarizes your answers to the following questions:

1. What are botnets and how do they work?
2. What features do the most popular botnets offer?
3. How does a bot infect and control a host computer?
4. How can a bot attack be prevented?

TABLE 7.2

Examples of Computer Crime

COMPUTERS AS TARGETS OF CRIME
Breaching the confidentiality of protected computerized data
Accessing a computer system without authority
Knowingly accessing a protected computer to commit fraud
Intentionally accessing a protected computer and causing damage, negligently or deliberately
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
Threatening to cause damage to a protected computer
COMPUTERS AS INSTRUMENTS OF CRIME
Theft of trade secrets
Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Schemes to defraud
Using e-mail for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including e-mail and voice mail
Transmitting or possessing child pornography using a computer

Identify theft has flourished on the Internet, with credit card files a major target of Web site hackers. Moreover, e-commerce sites are wonderful sources of customer personal information—name, address, and phone number. Armed with this information, criminals are able to assume new identities and establish new credit for their own purposes.

One increasingly popular tactic is a form of spoofing called **phishing**. Phishing involves setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data. The e-mail message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering the information at a bogus Web site, or by calling a telephone number. In October 2007, the OpenDNS PhishTank Annual Report found that the top two spoofed brands were eBay and PayPal, with a variety of banks, the IRS, and several large retailers (Amazon and Wal-Mart) rounding out the top 10 (OpenDNS, 2007).

New phishing techniques called evil twins and pharming are harder to detect. **Evil twins** are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airport lounges, hotels, or coffee shops. The bogus network looks identical to a legitimate public network. Fraudsters try to capture passwords or credit card numbers of unwitting users who log on to the network.

Pharming redirects users to a bogus Web page, even when the individual types the correct Web page address into his or her browser. This is possible if pharming perpetrators gain access to the Internet address information stored by Internet service providers to speed up Web browsing and the ISP companies have flawed software on their servers that allows the fraudsters to hack in and change those addresses.

The U.S. Congress addressed the threat of computer crime in 1986 with the Computer Fraud and Abuse Act. This act makes it illegal to access a computer system without authorization. Most states have similar laws, and nations in Europe have comparable legislation. Congress also passed the National Information Infrastructure Protection Act in 1996 to make virus distribution and hacker attacks to disable Web sites federal crimes. U.S. legislation, such as the Wiretap Act, Wire Fraud Act, Economic Espionage Act, Electronic Communications Privacy Act, E-Mail Threats and Harassment Act, and Child Pornography Act, covers computer crimes involving intercepting electronic communication, using electronic communication to defraud, stealing trade secrets, illegally accessing stored electronic communications, using e-mail for threats or harassment, and transmitting or possessing child pornography.

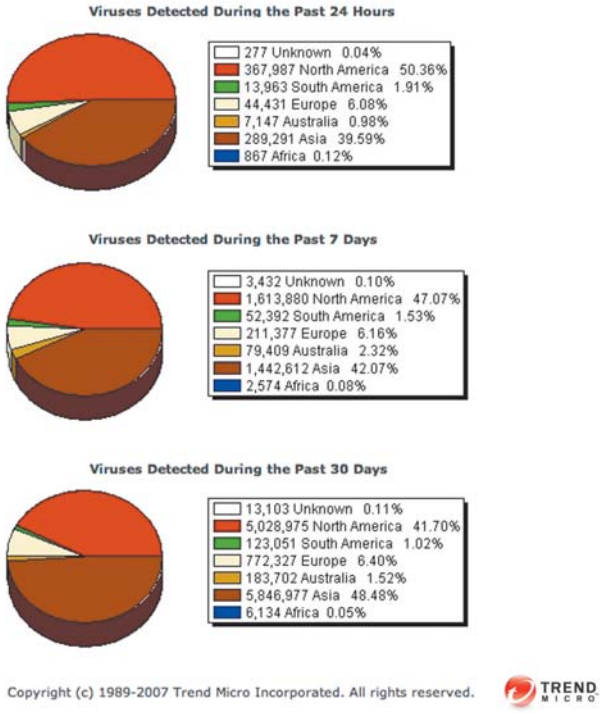
Click Fraud

When you click on an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its products. **Click fraud** occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising (see the case study concluding Chapter 6.)

Some companies hire third parties (typically from low-wage countries) to fraudulently click on a competitor's ads to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking, and bot networks are often used for this purpose (review the Interactive Session on Technology). Search engines such as Google attempt to monitor click fraud but have been reluctant to publicize their efforts to deal with the problem.

Global Threats: Cyberterrorism and Cyberwarfare

The cybercriminal activities we have described—launching malware, bot networks, DoS attacks, and phishing probes—are borderless. Computer security firm Sophos reported that 34.2 percent of the malware it identified in 2006 originated in the United States, while 31



Malware is active throughout the globe. These three charts show the regional distribution of worms and computer viruses worldwide reported by Trend Micro over periods of 24 hours, 7 days, and 30 days. The virus count represents the number of infected files and the percentage shows the relative prevalence in each region compared to worldwide statistics for each measuring period.

percent came from China, and 9.5 percent from Russia (Australian IT News, 2007). The global nature of the Internet makes it possible for cybercriminals to operate—and to do harm—anywhere in the world.

Concern is mounting that the vulnerabilities of the Internet or other networks make digital networks targets for digital attacks by terrorists, foreign intelligence services, or other groups seeking to create widespread disruption and harm. Such cyberattacks might target the software that runs electrical power grids, air traffic control systems, or networks of major banks and financial institutions. At least 20 countries, including China, are believed to be developing offensive and defensive cyberwarfare capabilities. U.S. military networks and U.S. government agencies suffer hundreds of hacker attacks each year.

To deal with this threat, the U.S. Department of Homeland Security (DHS) has been charged with orchestrating activities to support critical information systems that safeguard critical infrastructures in the United States. Its responsibilities include promoting public and private information sharing about cyberattacks, threats, and vulnerabilities; developing national cyberanalysis and warning capabilities; incorporating cybersecurity into a comprehensive national plan for critical infrastructure protection; and coordinating with government and private sector groups to respond to cyberevents. The U.S. Department of Defense has joint task forces for computer network defense and for managing computer network attacks.

INTERNAL THREATS: EMPLOYEES

We tend to think the security threats to a business originate outside the organization. In fact, company insiders pose serious security problems. Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace.

Studies have found that user lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or

allow co-workers to use them, which compromises the system. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called **social engineering**.

Both end users and information systems specialists are also a major source of errors introduced into information systems. End users introduce errors by entering faulty data or by not following the proper instructions for processing data and using computer equipment. Information systems specialists may create software errors as they design and develop new software or maintain existing programs.

SOFTWARE VULNERABILITY

Software errors pose a constant threat to information systems, causing untold losses in productivity. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities. For example, a flawed software upgrade shut down the BlackBerry e-mail service throughout North America for about 12 hours between April 17 and April 18, 2007. Millions of business users who depended on BlackBerry were unable to work, and BlackBerry's reputation for reliability was tarnished (Martin, 2007). The U.S. Department of Commerce National Institute of Standards and Technology (NIST) reported that software flaws (including vulnerabilities to hackers and malware) cost the U.S. economy $59.6 billion each year (NIST, 2005).

A major problem with software is the presence of hidden **bugs** or program code defects. Studies have shown that it is virtually impossible to eliminate all bugs from large programs. The main source of bugs is the complexity of decision-making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of different paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

Zero defects cannot be achieved in larger programs. Complete testing simply is not possible. Fully testing programs that contain thousands of choices and millions of paths would require thousands of years. Even with rigorous testing, you would not know for sure that a piece of software was dependable until the product proved itself after much operational use.

Flaws in commercial software not only impede performance but also create security vulnerabilities that open networks to intruders. Each year, security firms identify about 5,000 software vulnerabilities in Internet and PC software. For instance, in 2007, Symantec identified 39 vulnerabilities in Microsoft Internet Explorer, 34 in Mozilla browsers, 25 in Apple Safari, and 7 in Opera. Some of these vulnerabilities are critical (Symantec, 2007).

To correct software flaws once they are identified, the software vendor creates small pieces of software called **patches** to repair the flaws without disturbing the proper operation of the software. An example is Microsoft's XP Service Pack 2 (SP2) introduced in 2004, which features added firewall protection against viruses and intruders, capabilities for automatic security updates, and an easy-to-use interface for managing the security applications on the user's computer. It is up to users of the software to track these vulnerabilities, test, and apply all patches. This process is called patch management.

Because a company's IT infrastructure is typically laden with multiple business applications, operating system installations, and other system services, maintaining patches on all devices and services used by a company is often time-consuming and costly. Malware is being created so rapidly that companies have very little time to respond between the time a vulnerability and a patch are announced and the time malicious software appears to exploit the vulnerability.

7.2 Business Value of Security and Control

Many firms are reluctant to spend heavily on security because it is not directly related to sales revenue. However, protecting information systems is so critical to the operation of the business that it deserves a second look.

Companies have very valuable information assets to protect. Systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They also can contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. Government systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands. One study estimated that when the security of a large firm is compromised, the company loses approximately 2.1 percent of its market value within two days of the security breach, which translates into an average loss of $1.65 billion in stock market value per incident (Cavusoglu, Mishra, and Raghunathan, 2004).

Inadequate security and control may result in serious legal liability. Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Failure to do so may open the firm to costly litigation for data exposure or theft. An organization can be held liable for needless risk and harm created if the organization fails to take appropriate protective action to prevent loss of confidential information, data corruption, or breach of privacy (see the chapter-ending case study). For example, B.J.'s Wholesale Club was sued by the U.S. Federal Trade Commission for allowing hackers to access its systems and steal credit and debit card data for fraudulent purchases. Banks that issued the cards with the stolen data sought $13 million from B.J.'s to compensate them for reimbursing card holders for the fraudulent purchases (McDougall, 2006). A sound security and control framework that protects business information assets can thus produce a high return on investment.

Strong security and control also increase employee productivity and lower operational costs. For example, Axia NextMedia Corp., a Calgary, Alberta firm that builds and manages open-access broadband networks, saw employee productivity go up and costs go down after it installed an information systems configuration and control system in 2004. Before then, Axia had lost valuable employee work time because of security or other network incidents that caused system outages. Between 2004 and 2007, the new configuration and control system saved the company $590,000 by minimizing system outages (Bartholomew, 2007).

LEGAL AND REGULATORY REQUIREMENTS FOR ELECTRONIC RECORDS MANAGEMENT

Recent U.S. government regulations are forcing companies to take security and control more seriously by mandating the protection of data from abuse, exposure, and unauthorized access. Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection.

If you work in the healthcare industry, your firm will need to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. **HIPAA** outlines medical security and privacy rules and procedures for simplifying the administration of healthcare billing and automating the transfer of healthcare data between healthcare providers, payers, and plans. It requires members of the healthcare industry to retain patient information for six years and ensure the confidentiality of those records. It specifies privacy, security, and electronic transaction standards for healthcare providers handling patient information, providing penalties for breaches of medical privacy, disclosure of patient records by e-mail, or unauthorized network access.

If you work in a firm providing financial services, your firm will need to comply with the **Gramm-Leach-Bliley Act**. The Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act after its congressional sponsors, requires financial

institutions to ensure the security and confidentiality of customer data. Data must be stored on a secure medium. Special security measures must be enforced to protect such data on storage media and during transmittal.

If you work in a publicly traded company, your company will need to comply with the **Sarbanes-Oxley Act**. The Public Company Accounting Reform and Investor Protection Act of 2002, better known as Sarbanes-Oxley after its sponsors Senator Paul Sarbanes of Maryland and Representative Michael Oxley of Ohio, was designed to protect investors after the financial scandals at Enron, WorldCom, and other public companies. It imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally. One of the Learning Tracks for this chapter discusses Sarbanes-Oxley in detail.

Sarbanes-Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Because information systems are used to generate, store, and transport such data, the legislation requires firms to consider information systems security and other controls required to ensure the integrity, confidentiality, and accuracy of their data. Each system application that deals with critical financial reporting data requires controls to make sure the data are accurate. Controls to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the event of disaster or other disruption of service are essential as well.

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. In addition to information from printed or typewritten pages, legal cases today increasingly rely on evidence represented as digital data stored on portable floppy disks, CDs, and computer hard disk drives, as well as in e-mail, instant messages, and e-commerce transactions over the Internet. E-mail is currently the most common type of electronic evidence.

In a legal action, a firm is obligated to respond to a discovery request for access to information that may be used as evidence, and the company is required by law to produce those data. The cost of responding to a discovery request can be enormous if the company has trouble assembling the required data or the data have been corrupted or destroyed. Courts now impose severe financial and even criminal penalties for improper destruction of electronic documents.

An effective electronic document retention policy ensures that electronic documents, e-mail, and other records are well organized and accessible, and neither retained too long nor discarded too soon. It also reflects an awareness of how to preserve potential evidence for computer forensics. **Computer forensics** is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. It deals with the following problems:

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

Electronic evidence may reside on computer storage media in the form of computer files and as *ambient data*, which are not visible to the average user. An example might be a file that has been deleted on a PC hard drive. Data that a computer user may have deleted on computer storage media can be recovered through various techniques. Computer forensics experts try to recover such hidden data for presentation as evidence.

An awareness of computer forensics should be incorporated into a firm's contingency planning process. The CIO, security specialists, information systems staff, and corporate legal counsel should all work together to have a plan in place that can be executed if a legal need arises. You can find out more about computer forensics in a Learning Track for this chapter.

7.3 Establishing a Framework for Security and Control

Even with the best security tools, your information systems won't be reliable and secure unless you know how and where to deploy them. You will need to know where your company is at risk and what controls you must have in place to protect your information systems. You will also need to develop a security policy and plans for keeping your business running if your information systems aren't operational.

INFORMATION SYSTEMS CONTROLS

Information systems controls are both manual and automated and consist of both general controls and application controls. **General controls** govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems implementation process, and administrative controls. Table 7.3 describes the functions of each of these controls.

TABLE 7.3
General Controls

Type of General Control	Description
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalized standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Application controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.

Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling. Processing controls establish that data are complete and accurate during updating. Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. You can find more detail about application and general controls in our Learning Tracks.

RISK ASSESSMENT

Before your company commits resources to security and information systems controls, it must know which assets require protection and the extent to which these assets are vulnerable. A risk assessment helps answer these questions and determine the most cost-effective set of controls for protecting assets.

A **risk assessment** determines the level of risk to the firm if a specific activity or process is not properly controlled. Business managers working with information systems specialists can determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. For example, if an event is likely to occur no more than once a year, with a maximum $1,000 loss to the organization, it is not feasible to spend $20,000 on the design and maintenance of a control to protect against that event. However, if that same event could occur at least once a day, with a potential loss of more than $300,000 a year, $100,000 spent on a control might be entirely appropriate.

Table 7.4 illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an average loss calculated by adding the highest and lowest figures together and dividing by two. The expected annual loss for each exposure can be determined by multiplying the average loss by its probability of occurrence.

This risk assessment shows that the probability of a power failure occurring in a one-year period is 30 percent. Loss of order transactions while power is down could range from $5,000 to $200,000 (averaging $102,500) for each occurrence, depending on how long processing is halted. The probability of embezzlement occurring over a yearly period is about 5 percent, with potential losses ranging from $1,000 to $50,000 (and averaging $25,500) for each occurrence. User errors have a 98-percent chance of occurring over a yearly period, with losses ranging from $200 to $40,000 (and averaging $20,100) for each occurrence.

Once the risks have been assessed, system builders will concentrate on the control points with the greatest vulnerability and potential for loss. In this case, controls should focus on ways to minimize the risk of power failures and user errors because anticipated annual losses are highest for these areas.

TABLE 7.4

Online Order Processing Risk Assessment

Exposure	Probability of Occurrence (%)	Loss Range/ Average ($)	Expected Annual Loss ($)
Power failure	30%	$5,000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000–$50,000 ($25,500)	$1,275
User error	98%	$200–$40,000 ($20,100)	$19,698

SECURITY POLICY

Once you have identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets. A **security policy** consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. What are the firm's most important information assets? Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What level of risk is management willing to accept for each of these assets? Is it willing, for instance, to lose customer credit data once every 10 years? Or will it build a security system for credit card data that can withstand the once-in-a-100-year disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

The security policy drives policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An **acceptable use policy (AUP)** defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance. For example, security policy at Unilever, the giant multinational consumer goods company, requires every employee equipped with a laptop or mobile handheld device to use a company-specified device and employ a password or other method of identification when logging onto the corporate network.

Authorization policies determine differing levels of access to information assets for different levels of users. **Authorization management systems** establish where and when a user is permitted to access certain parts of a Web site or a corporate database. Such systems allow each user access only to those portions of a system that person is permitted to enter, based on information established by a set of access rules.

The authorization management system knows exactly what information each user is permitted to access, as shown in Figure 7-3. This figure illustrates the security allowed for two sets of users of an online personnel database containing sensitive information, such as employees' salaries, benefits, and medical histories. One set of users consists of all employees who perform clerical functions, such as inputting employee data into the system. All individuals with this type of profile can update the system but can neither read nor update sensitive fields, such as salary, medical history, or earnings data. Another profile applies to a divisional manager, who cannot update the system but who can read all employee data fields for his or her division, including medical history and salary. These profiles are based on access rules supplied by business groups. The system illustrated in Figure 7-3 provides very fine-grained security restrictions, such as allowing authorized personnel users to inquire about all employee information except that in confidential fields, such as salary or medical history.

DISASTER RECOVERY PLANNING AND BUSINESS CONTINUITY PLANNING

If you run a business, you need to plan for events, such as power outages, floods, earthquakes, or terrorist attacks that will prevent your information systems and your business from operating. **Disaster recovery planning** devises plans for the restoration of computing and communications services after they have been disrupted. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

For example, MasterCard maintains a duplicate computer center in Kansas City, Missouri, to serve as an emergency backup to its primary computer center in St. Louis. Rather than build their own backup facilities, many firms contract with disaster recovery firms, such as Comdisco Disaster Recovery Services in Rosemont, Illinois, and SunGard

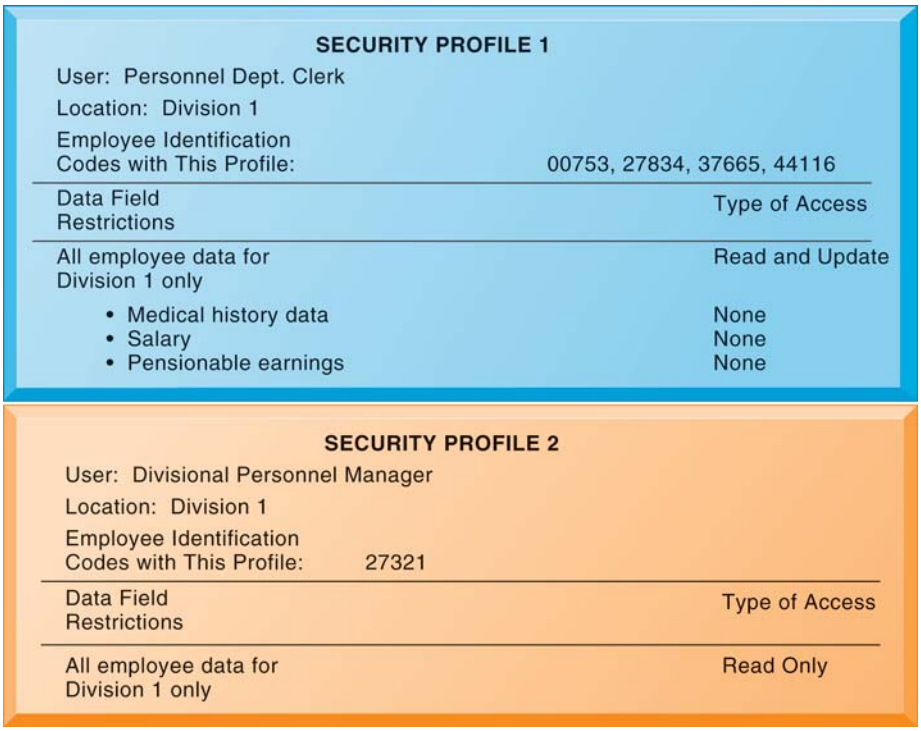


Figure 7-3
Security Profiles for a Personnel System
These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

Availability Services, headquartered in Wayne, Pennsylvania. These disaster recovery firms provide hot sites housing spare computers at locations around the country where subscribing firms can run their critical applications in an emergency. For example, Champion Technologies, which supplies chemicals used in oil and gas operations, is able to switch its enterprise systems from Houston to a SunGard hot site in Scottsdale, Arizona in two hours (Duvall, 2007).

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down. For example, Deutsche Bank, which provides investment banking and asset management services in 74 different countries, has a well-developed business continuity plan that it continually updates and refines. It maintains full-time teams in Singapore, Hong Kong, Japan, India, and Australia to coordinate plans addressing loss of facilities, personnel, or critical systems so that the company can continue to operate when a catastrophic event occurs. Deutsche Bank's plan distinguishes between processes critical for business survival and those critical to crisis support and is coordinated with the company's disaster recovery planning for its computer centers.

Business managers and information technology specialists need to work together on both types of plans to determine which systems and business processes are most critical to the company. They must conduct a business impact analysis to identify the firm's most critical systems and the impact a systems outage would have on the business. Management must determine the maximum amount of time the business can survive with its systems down and which parts of the business must be restored first.

THE ROLE OF AUDITING

How does management know that information systems security and controls are effective? To answer this question, organizations must conduct comprehensive and systematic audits. An **MIS audit** examines the firm's overall security environment as well as controls governing individual information systems. The auditor should trace the flow of sample transactions through the system and perform tests, using, if appropriate,

Function: Loans Location: Peoria, IL	Prepared by: J. Ericson Date: June 16, 2008		Received by: T. Benson Review date: June 28, 2008	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/08	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/08	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Figure 7-4
Sample Auditor's List of Control Weaknesses
This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

automated audit software. The MIS audit may also examine data quality, as described in Chapter 5.

Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. Figure 7-4 is a sample auditor's listing of control weaknesses for a loan system. It includes a section for notifying management of such weaknesses and for management's response. Management is expected to devise a plan for countering significant weaknesses in controls.

7.4 Technologies and Tools for Protecting Information Resources

Businesses have an array of tools and technologies for protecting their information resources. They include tools and technologies for securing systems and data, ensuring system availability, and ensuring software quality.

ACCESS CONTROL

Access control consists of all the policies and procedures a company uses to prevent improper access to systems by unauthorized insiders and outsiders. To gain access a user must be authorized and authenticated. **Authentication** refers to the ability to know that a person is who he or she claims to be. Access control software is designed to allow only authorized users to use systems or to access data using some method for authentication.

Authentication is often established by using passwords known only to authorized users. An end user uses a password to log on to a computer system and may also use passwords for accessing specific systems and files. However, users often forget passwords, share them, or choose poor passwords that are easy to guess, which compromises security. Password systems that are too rigorous hinder employee productivity. When employees must change complex passwords frequently, they often take shortcuts, such as choosing passwords that are

easy to guess or writing down their passwords at their workstations in plain view. Passwords can also be "sniffed" if transmitted over a network or stolen through social engineering.

New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. A **token** is a physical device, similar to an identification card, that is designed to prove the identity of a single user. Tokens are small gadgets that typically fit on key rings and display passcodes that change frequently. A **smart card** is a device about the size of a credit card that contains a chip formatted with access permission and other data. (Smart cards are also used in electronic payment systems.) A reader device interprets the data on the smart card and allows or denies access.

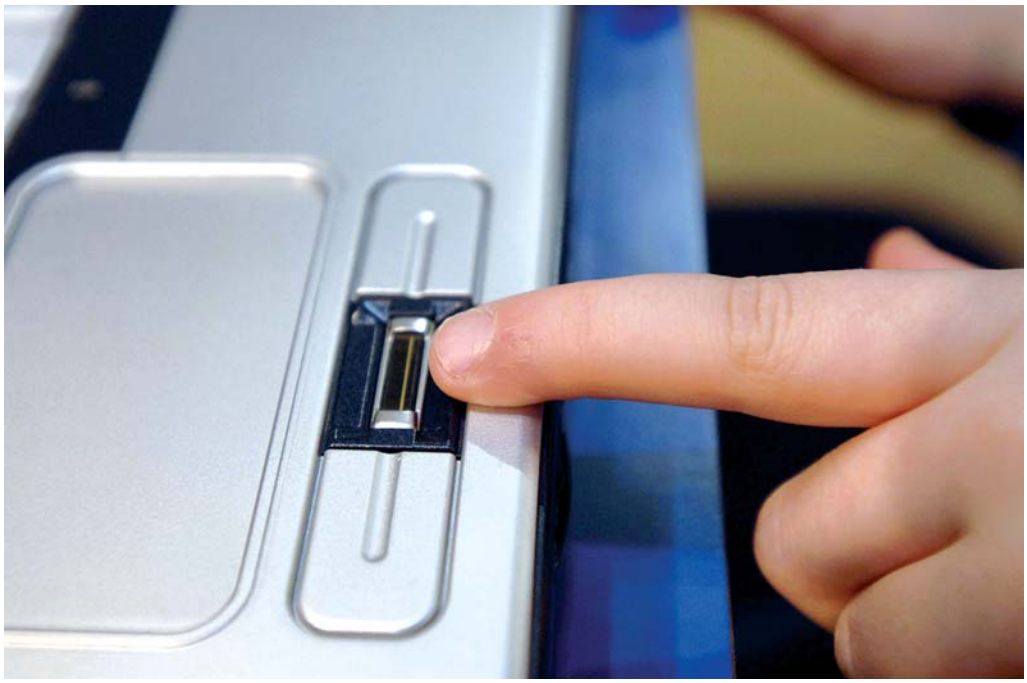
Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices, in order to grant or deny access. Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored set profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. If the two profiles match, access is granted. Fingerprint and facial recognition technologies are just beginning to be used for security applications. About 10 percent of all new laptops sold in the United States come equipped with fingerprint identification devices.

FIREWALLS, INTRUSION DETECTION SYSTEMS, AND ANTIVIRUS SOFTWARE

Without protection against malware and intruders, connecting to the Internet would be very dangerous. Firewalls, intrusion detection systems, and antivirus software have become essential business tools.

Firewalls

Chapter 6 describes the use of *firewalls* to prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network (see Figure 7-5).



This NEC PC has a biometric fingerprint reader for fast yet secure access to files and networks. New models of PCs are starting to use biometric identification to authenticate users.

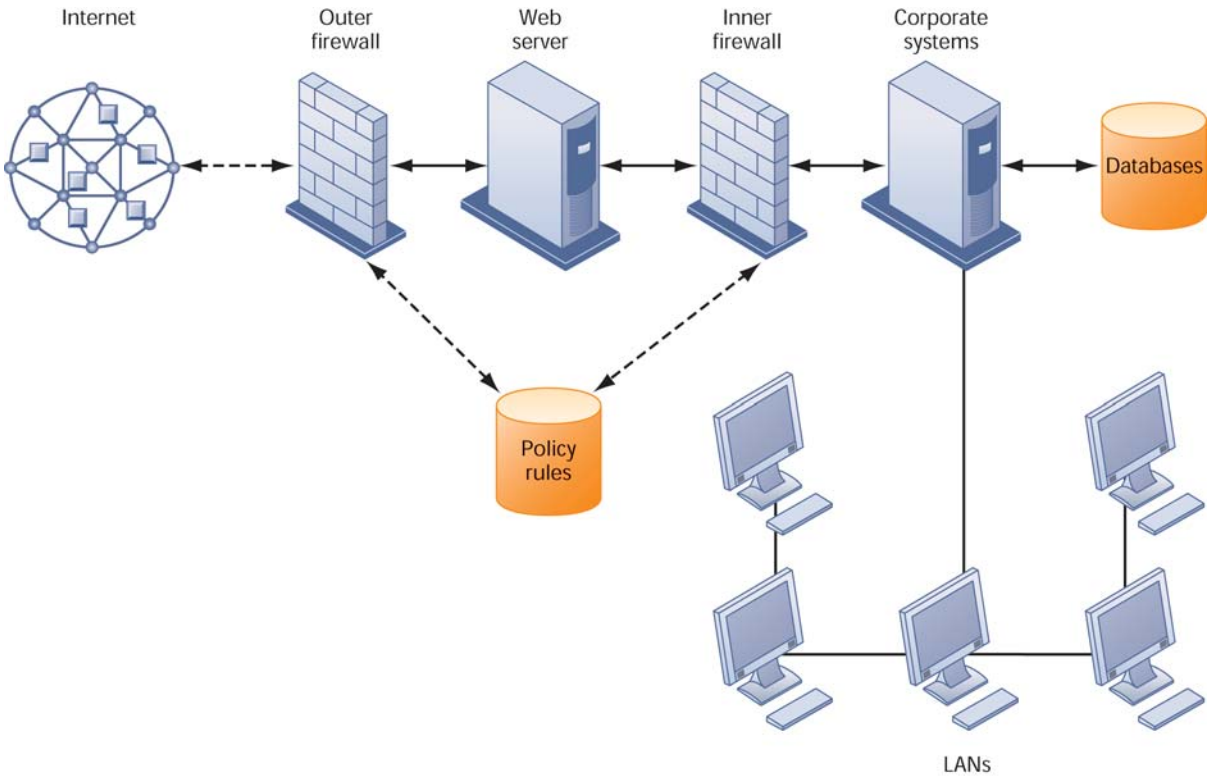


Figure 7-5
A Corporate Firewall
The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

The firewall acts like a gatekeeper who examines each user's credentials before access is granted to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed into the system by the network administrator. The firewall prevents unauthorized communication into and out of the network.

In large organizations, the firewall often resides on a specially designated computer separate from the rest of the network, so no incoming request directly accesses private network resources. There are a number of firewall screening technologies, including static packet filtering, stateful inspection, Network Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection.

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks. *Stateful inspection* provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or whether they are attempting to establish a legitimate connection.

Network Address Translation (NAT) can provide another layer of protection when static packet filtering and stateful inspection are employed. NAT conceals the IP addresses of the organization's internal host computer(s) to prevent sniffer programs outside the firewall from ascertaining them and using that information to penetrate internal systems.

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate

with a user inside the organization, the outside user first "talks" to the proxy application and the proxy application communicates with the firm's internal computer. Likewise, a computer user inside the organization goes through the proxy to talk with computers on the outside.

To create a good firewall, an administrator must maintain detailed internal rules identifying the people, applications, or addresses that are allowed or rejected. Firewalls can deter, but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan.

Intrusion Detection Systems

In addition to firewalls, commercial security vendors now provide intrusion detection tools and services to protect against suspicious network traffic and attempts to access files and databases. **Intrusion detection systems** feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually. The system generates an alarm if it finds a suspicious or anomalous event. Scanning software looks for patterns indicative of known methods of computer attacks, such as bad passwords, checks to see if important files have been removed or modified, and sends warnings of vandalism or system administration errors. Monitoring software examines events as they are happening to discover security attacks in progress. The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Antivirus and Antispyware Software

Defensive technology plans for both individuals and businesses must include antivirus protection for every computer. **Antivirus software** is designed to check computer systems and drives for the presence of computer viruses and worms. Often the software eliminates the virus from the infected area. However, most antivirus software is effective only against malware already known when the software was written. To remain effective, the antivirus software must be continually updated. Antivirus products are available for mobile and handheld devices.

Leading antivirus software vendors, such as McAfee, Symantec and Trend Micro, have enhanced their products to include protection against spyware. Anti-spyware software tools such as Ad-Aware, Spybot, and Spyware Doctor are also very helpful.

SECURING WIRELESS NETWORKS

Despite its flaws, WEP provides some margin of security if Wi-Fi users remember to activate it. A simple first step to thwart hackers is to assign a unique name to your network's SSID and instruct your router not to broadcast it. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

In June 2004, the Wi-Fi Alliance industry trade group finalized the 802.11i specification (also referred to as Wi-Fi Protected Access 2 or WAP2) that replaces WEP with stronger security standards. Instead of the static encryption keys used in WEP, the new standard uses much longer keys that continually change, making them harder to crack. It also employs an encrypted authentication system with a central authentication server to ensure that only authorized users access the network.

ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE

Many businesses use encryption to protect digital information that they store, physically transfer, or send over the Internet. **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver. Data are encrypted by using a secret numerical code, called an encryption key, that transforms plain data into cipher text. The message must be decrypted by the receiver.

Two methods for encrypting network traffic on the Web are SSL and S-HTTP. **Secure Sockets Layer (SSL)** and its successor Transport Layer Security (TLS) enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. **Secure Hypertext Transfer Protocol (S-HTTP)** is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages, whereas SSL and TLS are designed to establish a secure connection between two computers.

The capability to generate secure sessions is built into Internet client browser software and servers. The client and the server negotiate what key and what level of security to use. Once a secure session is established between the client and the server, all messages in that session are encrypted.

There are two alternative methods of encryption: symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length. Today, a typical key will be 128 bits long (a string of 128 binary digits).

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might be able to intercept and decrypt the key. A more secure form of encryption called **public key encryption** uses two keys: one shared (or public) and one totally private as shown in Figure 7-6. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions (see Figure 7-7). A digital certificate system uses a trusted third party, known as a certification authority (CA), to validate a user's identity. There are many CAs in the United States and around the world, including VeriSign, IdenTrust, and Australia's KeyPost. The CA verifies a digital certificate user's identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner's public key. The certificate authenticates that the public key belongs to the designated owner. The CA makes its own public key available publicly either in print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it was issued by the CA, and then obtains the sender's public key and identification information contained in the certificate. Using this information, the recipient can send an encrypted reply. The digital certificate system would enable, for exam-

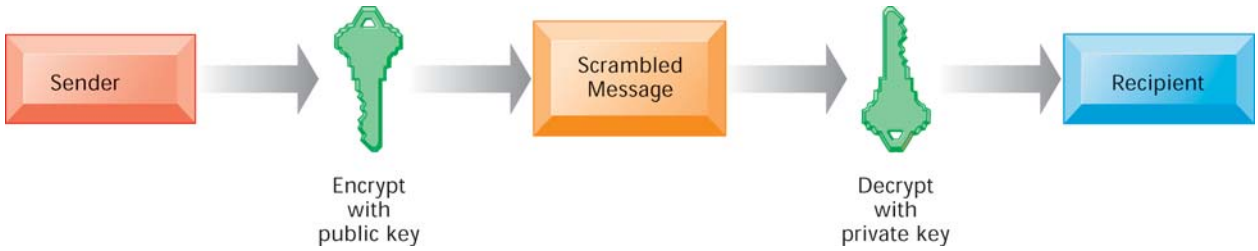


Figure 7-6
Public Key Encryption
A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

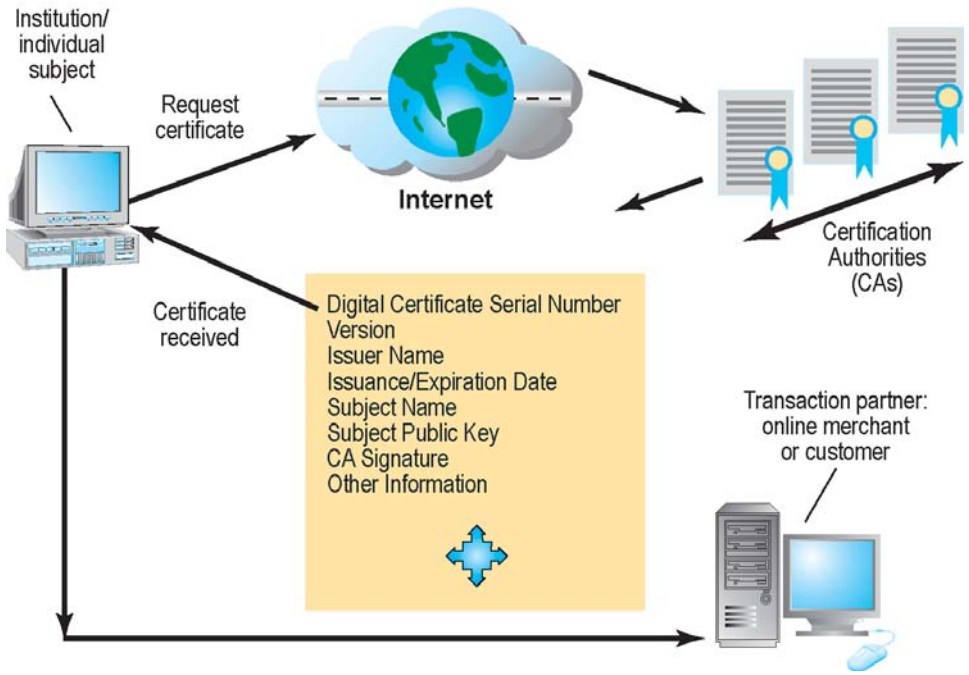


Figure 7-7
Digital Certificates
Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

ple, a credit card user and a merchant to validate that their digital certificates were issued by an authorized and trusted third party before they exchange data. **Public key infrastructure (PKI)**, the use of public key cryptography working with a certificate authority, is now widely used in e-commerce.

ENSURING SYSTEM AVAILABILITY

As companies increasingly rely on digital networks for revenue and operations, they need to take additional steps to ensure that their systems and applications are always available. Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100-percent availability. In **online transaction processing**, transactions entered online are immediately processed by the computer. Multitudinous changes to databases, reporting, and requests for information occur each instant.

Fault-tolerant computer systems contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. Parts from these computers can be removed and repaired without disruption to the computer system.

Fault tolerance should be distinguished from **high-availability computing**. Both fault tolerance and high-availability computing try to minimize downtime. **Downtime** refers to periods of time in which a system is not operational. However, high-availability computing helps firms recover quickly from a system crash, whereas fault tolerance promises continuous availability and the elimination of recovery time altogether.

High-availability computing environments are a minimum requirement for firms with heavy electronic commerce processing or for firms that depend on digital networks for their internal operations. High-availability computing requires backup servers, distribution of processing across multiple servers, high-capacity storage, and good disaster recovery and business continuity plans. The firm's computing platform must be extremely robust with scalable processing power, storage, and bandwidth.

Researchers are exploring ways to make computing systems recover even more rapidly when mishaps occur, an approach called **recovery-oriented computing**. This work includes designing systems that recover quickly, and implementing capabilities and tools to help operators pinpoint the sources of faults in multi-component systems and easily correct their mistakes.

The Interactive Session on Organizations describes the efforts of Salesforce.com to make sure its systems are always available to subscribers. Salesforce.com is a Web-based on-demand customer relationship management (CRM) and business services provider. Companies subscribing to its service use Salesforce.com's software programs running on Salesforce's servers. If Salesforce.com's services fail, they can't run their CRM applications. That's exactly what happened when Salesforce.com was hit by a series of service outages in late 2005 and 2006. As you read this case, try to identify the problem Salesforce.com encountered; what alternative solutions were available to management; and the people, organization, and technology issues that had to be addressed when developing the solution.

Controlling Network Traffic: Deep Packet Inspection

Have you ever tried to use your campus network and found it was very slow? It may be because your fellow students are using the network to download music or watch YouTube. Bandwith-consuming applications such as file-sharing programs, Internet phone service, and online video, are able to clog and slow down corporate networks, degrading performance. For example, Ball Sate University in Muncie, Indiana found its network had slowed because a small minority of students were using peer-to-peer file sharing programs to download movies and music.

A technology called **deep packet inspection (DPI)** helps solve this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds. Using a DPI system from Allot Communications, Ball State was able to cap the amount of file-sharing traffic and assign it a much lower priority. Ball State's preferred network traffic speeded up (White, 2007).

Security Outsourcing

Many companies, especially small businesses, lack the resources or expertise to provide a secure high-availability computing environment on their own. They can outsource many security functions to **managed security service providers (MSSPs)** that monitor network activity and perform vulnerability testing and intrusion detection. Guardent, Counterpane, VeriSign, and Symantec are leading providers of MSSP services.

ENSURING SOFTWARE QUALITY

In addition to implementing effective security and controls, organizations can improve system quality and reliability by employing software metrics and rigorous software testing. Software metrics are objective assessments of the system in the form of quantified measurements. Ongoing use of metrics allows the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples of software metrics include the number of transactions that can be processed in a specified unit of time, online response time, the number of payroll checks printed per hour, and the number of known bugs per hundred lines of program code. For metrics to be successful, they must be carefully designed, formal, objective, and used consistently.

Early, regular, and thorough testing will contribute significantly to system quality. Many view testing as a way to prove the correctness of work they have done. In fact, we know that all sizable software is riddled with errors, and we must test to uncover these errors.

INTERACTIVE SESSION: ORGANIZATIONS Can Salesforce.com On-Demand Remain in Demand?

Salesforce.com, headquartered in San Francisco, California, is the worldwide leader in on-demand customer relationship management (CRM) services. It offers hosted applications that manage customer information for sales, marketing, and customer support. Companies used Salesforce.com's applications for generating sales leads, maintaining customer records, and tracking customer interactions. As of January 31, 2007, Salesforce.com had about 29,800 customers and 646,000 paying subscriptions worldwide. More companies trust their vital customer and sales data to Salesforce.com than to any other on-demand CRM company in the world.

Imagine then, the impact if Salesforce.com's services are not available. That's exactly what happened during a six-week period in late 2005 and early 2006. Starting on December 20, 2005, Salesforce.com clients could not access the company's servers and obtain their customer records for more than three hours. A rare database software bug was the source of the problem. Oracle Database 10g and Oracle Grid Computing are key technologies for Salesforce.com's service and internal operations, and these tools are considered among the best in the business. Salesforce.com was careful not to blame Oracle for the outage, and instead focused on working with Oracle to eradicate the bug. It has not resurfaced since the initial occurrence. But with no access to customers' records, some businesses came to a standstill for the duration of the outage.

Salesforce.com experienced two more outages in January and several in early February attributed to "system performance issues." A January 30 performance problem was traced to a shortcoming in the company's database cluster, or collection of databases. Salesforce.com had to restart each database instance in the cluster, interrupting service to do so. Its service was down for about four hours. Even when the service was brought back up, its application programming interface was disabled for a few more hours.

On February 9, 2006, a primary hardware server failed and one of the company's four North American servers did not automatically recover. Salesforce.com had to restart the database running on this server manually. The outage lasted slightly more than one hour.

These service outages could not have occurred at a worse time. Salesforce.com was growing rapidly and seeking to attract more large customers with new software and services in addition to CRM. In January 2006, it launched AppExchange, an online marketplace for applications and Web services from other vendors and developers that can be customized and integrated with Salesforce.com's CRM service. Salesforce.com would not be able to convince enterprise customers to let it run their applications if it could not guarantee that that its services were 100-percent reliable.

The outages caused some clients and analysts to ask whether Salesforce.com had run into capacity or scalability problems. At the time of the first incident, analysts agreed that a one-time outage would not cause a crisis of confidence on the part of clients. Many clients admitted that Salesforce.com had a better record of maintaining uptime than the clients' own companies did. What was of more concern to some clients was the failure of Salesforce.com to communicate adequately with its clients about the outage. They were left in the dark as to what exactly was happening with the on-demand service. At least one client (Mission Research, a Lancaster, Pennsylvania developer of fund-raising software) dropped Salesforce.com in favor of an internal system immediately on December 20, 2005.

In the weeks that followed that outage, it became apparent that the problems at Salesforce.com were not limited to a software bug. The recurring outages raised doubts about the fidelity of the service's infrastructure as a whole. These outages coincided with the end of the month and, for some companies, the end of the fiscal year. It was an extraordinarily inconvenient time to lose access to customer data.

The complaints from clients grew louder. They focused not only on the failure of the on-demand service but on poor customer service and a tepid response from Salesforce.com management. One particularly outraged client created a blog at gripeforce.blogspot.com to express his dissatisfaction with the service. The blogger, CRMGuy, described salespeople at Salesforce.com as arrogant and customer service representatives as interested only in selling more user licenses. Salesforce.com's CEO, Mark Benioff, was roundly criticized for downplaying the interruptions as minor. "Having the company's CEO minimize an outage that brings customer businesses to a halt as a 'minor issue' is not acceptable." Of course, there were plenty of clients who found the increasing downtime unacceptable as well.

Salesforce.com moved quickly to improve its client communication. The company used direct communications and customer support outlets to update clients on efforts to resolve service problems. By the end of February 2006, Salesforce.com had launched Trust.Salesforce.com, a Web site that

displayed both real-time and historical data related to the performance of all key system components for its services. The site provided a measure of transparency into the level of database and service performance that clients were receiving, which they valued. Trust.Salesforce.com logs specific metrics, such as API transactions and page views. The site also gives general conditions using a color scheme to indicate service status for network nodes: green for OK, yellow for a performance issue, and red for an outage.

Even prior to the outages, Salesforce.com had been building up and redesigning its infrastructure to ensure better service. The company invested $50 million in Mirrorforce technology, a mirroring system that creates a duplicate database in a separate location and synchronizes the data instantaneously. If one database is disabled, the other takes over. Salesforce.com added two data centers on the East and West coasts in addition to its Silicon Valley facility and built an additional West Coast facility to support new product development. The company distributed processing for its larger customers among these centers to balance its database load. The investment in Mirrorforce necessitated a complete overhaul of Salesforce.com's hardware and software.

Salesforce.com's accelerated growth and switch to the new data centers had contributed to the outages. But by March 2006, Salesforce.com had strengthened its IT infrastructure to the point where outages were no longer occurring. Salesforce.com stated that it already met availability standards of 99-percent uptime in 2005 and 2006, but it was still striving to achieve 99.999-percent availability. On the public relations front, spokesman Bruce Francis offered an apology and recognition of clients' frustrations. Francis said, "There's no such thing as a minor outage because we know that even one moment of degraded availability is a moment our customers can't do what they need to do."

Sources: Laton McCartney, "Salesforce.com: When On-Demand Goes Off," *Baseline Magazine*, January 7, 2007; John Pallatto, "Rare Database Bug Causes Salesforce.com Outage," eWeek.com, December 22, 2005 and "Salesforce.com Confirms 'Minor' CRM Outage," eWeek.com, January 6, 2006; Alorie Gilbert, "Salesforce.com Users Lament Ongoing Outages," cnet News.com, February 1, 2006; and Bill Snyder, "Salesforce.com Outage Strikes Again," TheStreet.com, January 6, 2006.

CASE STUDY QUESTIONS

1. How did the problems experienced by Salesforce.com impact its business?
2. How did the problems impact its customers?
3. What steps did Salesforce.com take to solve the problems? Were these steps sufficient?
4. List and describe other vulnerabilities discussed in this chapter that might create outages at Salesforce.com and measures to safeguard against them.

MIS IN ACTION

Go to www.salesforce.com, reviewing the sections on Security, Availability, Performance, and Scalability. Then answer the following questions:

1. How does Saleforce.com deliver world-class security at the application, facilities, and network level?
2. What provisions does Salesforce.com have in place for disaster recovery and availability?
3. Click on trust.salesforce.com. What kinds of performance metrics does it display?
4. If you ran a business, would you feel confident about using Salesforce.com's on-demand service? Why or why not?

Good testing begins before a software program is even written by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. Once developers start writing software programs, coding walkthroughs also can be used to review program code. However, code must be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called *debugging*. You can find out more about the various stages of testing required to put an information system into operation in Chapter 11. Our Learning Tracks also contain descriptions of methodologies for developing software programs that also contribute to software quality.

7.5 Hands-On MIS

The projects in this section give you hands-on experience developing a disaster recovery plan, using spreadsheet software for risk analysis, and using Web tools to research security outsourcing services.

ACHIEVING OPERATIONAL EXCELLENCE: DEVELOPING A DISASTER RECOVERY PLAN

Software skills: Web browser and presentation software
Business skills: Disaster recovery planning

Management is concerned that Dirt Bikes's computer systems could be vulnerable to power outages, vandalism, computer viruses, natural disasters, or telecommunications disruptions. You have been asked to perform an analysis of system vulnerabilities and disaster recovery planning for the company. Your report should answer the following questions:

- What are the most likely threats to the continued operation of Dirt Bikes's systems?
- What would you identify as Dirt Bikes's most critical systems? What is the impact on the company if these systems cannot operate? How long could the company survive if these systems were down? Which systems are the most important to back up and restore in the event of a disaster?
- Use the Web to locate two disaster recovery services that could be used by a small business such as Dirt Bikes. Compare them in terms of the services they offer. Which should Dirt Bikes use? Exactly how could these services help Dirt Bikes recover from a disaster?
- (Optional) If possible use electronic presentation software to summarize your findings for management.

IMPROVING DECISION MAKING: USING SPREADSHEET SOFTWARE TO PERFORM A SECURITY RISK ASSESSMENT

Software skills: Spreadsheet formulas and charts
Business skills: Risk assessment

This project uses spreadsheet software to calculate anticipated annual losses from various security threats identified for a small company.

Mercer Paints is a small but highly regarded paint manufacturing company located in Alabama. The company has a network in place linking many of its business operations. Although the firm believes that its security is adequate, the recent addition of a Web site has become an open invitation to hackers. Management requested a risk assessment. The risk assessment identified a number of potential exposures. These exposures, their associated probabilities, and average losses are summarized in the following table.

Mercer Paints Risk Assessment

Exposure	Probability of Occurrence (%)	Average Loss ($)
Malware attack	60%	$75,000
Data loss	12%	$70,000
Embezzlement	3%	$30,000
User errors	95%	$25,000
Threats from hackers	95%	$90,000
Improper use by employees	5%	$5,000
Power failure	15%	$300,000

- In addition to the potential exposures listed, you should identify at least three other potential threats to Mercer Paints, assign probabilities, and estimate a loss range.
- Use spreadsheet software and the risk assessment data to calculate the expected annual loss for each exposure.
- Present your findings in the form of a chart. Which control points have the greatest vulnerability? What recommendations would you make to Mercer Paints? Prepare a written report that summarizes your findings and recommendations.

IMPROVING DECISION MAKING: EVALUATING SECURITY OUTSOURCING SERVICES

Software skills: Web browser and presentation software
Business skills: Evaluating business outsourcing services

Businesses today have a choice of whether to outsource the security function or maintain their own internal staff for this purpose. This project will help develop your Internet skills in using the Web to research and evaluate security outsourcing services.

As an information systems expert in your firm, you have been asked to help management decide whether to outsource security or keep the security function within the firm. Search the Web to find information to help you decide whether to outsource security and to locate security outsourcing services.

- Present a brief summary of the arguments for and against outsourcing computer security for your company.
- Select two firms that offer computer security outsourcing services, and compare them and their services.
- Prepare an electronic presentation for management summarizing your findings. Your presentation should make the case as to whether or not your company should outsource computer security. If you believe your company should outsource, the presentation should identify which security outsourcing service should be selected and justify your selection.

LEARNING TRACKS

The following Learning Tracks provide content relevant to topics covered in this chapter:

1. The Booming Job Market in IT Security
2. The Sarbanes-Oxley Act
3. Computer Forensics
4. General and Application Controls for Information Systems
5. Management Challenges of Security and Control

Review Summary

1 Why are information systems vulnerable to destruction, error, and abuse? Digital data are vulnerable to destruction, misuse, error, fraud, and hardware or software failures. The Internet is designed to be an open system and makes internal corporate systems more vulnerable to actions from outsiders. Hackers can unleash denial-of-service (DoS) attacks or penetrate corporate networks, causing serious system disruptions. Wi-Fi networks can be easily penetrated by intruders using sniffer programs to obtain an address to access the resources of the network. Computer viruses and worms can disable systems and Web sites. Software presents problems because software bugs may be impossible to eliminate and because software vulnerabilities can be exploited by hackers and malicious software. End users often introduce errors.

2 What is the business value of security and control? Lack of sound security and control can cause firms relying on computer systems for their core business functions to lose sales and productivity. Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability. New laws, such as HIPAA, the Sarbanes-Oxley Act, and the Gramm-Leach-Bliley Act, require companies to practice stringent electronic records management and adhere to strict standards for security, privacy, and control. Legal actions requiring electronic evidence and computer forensics also require firms to pay more attention to security and electronic records management.

3 What are the components of an organizational framework for security and control? Firms need to establish a good set of both general and application controls for their information systems. A risk assessment evaluates information assets, identifies control points and control weaknesses, and determines the most cost-effective set of controls. Firms must also develop a coherent corporate security policy and plans for continuing business operations in the event of disaster or disruption. The security policy includes policies for acceptable use and authorization. Comprehensive and systematic MIS auditing helps organizations determine the effectiveness of security and controls for their information systems.

4 What are the most important tools and technologies for safeguarding information resources? Firewalls prevent unauthorized users from accessing a private network when it is linked to the Internet. Intrusion detection systems monitor private networks from suspicious network traffic and attempts to access corporate systems. Passwords, tokens, smart cards, and biometric authentication are used to authenticate system users. Antivirus software checks computer systems for infections by viruses and worms and often eliminates the malicious software, while antispyware software combats intrusive and harmful spyware programs. Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over unprotected networks. Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user's identity. Companies can use fault-tolerant computer systems or create high-availability computing environments to make sure that their information systems are always available. Use of software metrics and rigorous software testing help improve software quality and reliability.

Key Terms

Acceptable use policy (AUP), 247
Access control, 249
Antivirus software, 252
Application controls, 246
Authentication, 249
Authorization management systems, 247
Authorization policies, 247
Biometric authentication, 250
Botnet, 237
Bugs, 242
Business continuity planning, 248
Click fraud, 240
Computer crime, 237
Computer forensics, 244
Computer virus, 234
Controls, 231
Cybervandalism, 236
Deep packet inspection (DPI), 255
Denial-of-service (DoS) attack, 237
Digital certificates, 253
Disaster recovery planning, 247
Distributed denial-of-service (DDoS) attack, 237
Downtime, 254
Encryption, 252
Evil twins, 240
Fault-tolerant computer systems, 254
General controls, 245
Gramm-Leach-Bliley Act, 243
Hacker, 236
High-availability computing, 254
HIPAA, 243
Identity theft, 237
Intrusion detection systems, 252
Key loggers, 236
Malware, 234
Managed security service providers (MSSPs), 255
MIS audit, 248
Online transaction processing, 254
Patches, 242

Pharming, 240
Phishing, 240
Public key encryption, 253
Public key infrastructure (PKI), 254
Recovery-oriented computing, 255
Risk assessment, 246
Sarbanes-Oxley Act, 244
Secure Hypertext Transfer Protocol (S-HTTP), 253
Secure Sockets Layer (SSL), 253
Security, 231
Security policy, 247
Smart card, 250
Sniffer, 236
Social engineering, 242
Spoofing, 236
Spyware, 236
Token, 250
Trojan horse, 236
War driving, 233
Worms, 234

Review Questions

1. Why are information systems vulnerable to destruction, error, and abuse?

- List and describe the most common threats against contemporary information systems.
- Define malware and distinguish among a virus, a worm, and a Trojan horse.
- Define a hacker and explain how hackers create security problems and damage systems.
- Define computer crime. Provide two examples of crime in which computers are targets and two examples in which computers are used as instruments of crime.
- Define identity theft and phishing and explain why identity theft is such a big problem today.
- Describe the security and system reliability problems created by employees.
- Explain how software defects affect system reliability and security.

2. What is the business value of security and control?

- Explain how security and control provide value for businesses.
- Describe the relationship between security and control and recent U.S. government regulatory requirements and computer forensics.

3. What are the components of an organizational framework for security and control?

- Define general controls and describe each type of general control.
- Define application controls and describe each type of application control.
- Describe the function of risk assessment and explain how it is conducted for information systems.
- Define and describe the following: security policy, acceptable use policy, authorization policy.
- Explain how MIS auditing promotes security and control.

4. What are the most important tools and technologies for safeguarding information resources?

- Name and describe three authentication methods.
- Describe the roles of firewalls, intrusion detection systems, and antivirus software in promoting security.
- Explain how encryption protects information.
- Describe the role of encryption and digital certificates in a public key infrastructure.
- Distinguish between fault-tolerant and high-availability computing, and between disaster recovery planning and business continuity planning.
- Describe measures for improving software quality and reliability.

Discussion Questions

1. Security isn't simply a technology issue, it's a business issue. Discuss.

2. If you were developing a business continuity plan for your company, where would you start? What aspects of the business would the plan address?

Video Case

You will find a video case illustrating some of the concepts in this chapter on the Laudon Web site along with questions to help you analyze the case.

Teamwork

Evaluating Security Software Tools

With a group of three or four students, use the Web to research and evaluate security products from two competing vendors, such as antivirus software, firewalls, or antispyware software. For each product, describe its capabilities, for what types of businesses it is best suited, and its cost to purchase and install. Which is the best product? Why? If possible, use electronic presentation software to present your findings to the class.

BUSINESS PROBLEM-SOLVING CASE

TXJ Companies' Credit Card Data Theft: The Worst Data Theft Ever?

Headquartered in Framingham, Massachusetts, TJX Companies is a $17 billion retailer with a global presence. The company's properties include 826 T.J. Maxx, 751 Marshalls, and 271 HomeGoods stores in the United States alone. On December 18, 2006, TJX management learned that its computer systems had been infiltrated by suspicious software, and intruders had stolen records with at least 45.7 million credit and debit card numbers. This is now the biggest known theft of credit card numbers in history. The TJX hackers also obtained personal information which could be used for identity theft, including driver license numbers, social security numbers, and military identification of 451,000 customers. The data theft took place over an eighteen-month period without anyone's knowledge.

How could this have happened? The thieves may have used several vulnerable entry points to TJX corporate systems. One was poorly secured computer kiosks located in many of TJX's retail stores, which let people apply for jobs electronically. These same kiosks also provide direct access to the company's internal corporate network. Hackers could have opened up the back of those terminals and inserted USB drives to install utility software that enabled them to turn the kiosks into remote terminals linked to TJX's networks. (The USB drives in the kiosks are normally used for plugging in mice or printers.) The TJX firewalls weren't set up to block malicious traffic coming from the kiosks.

Another entry point was wireless. The hackers may have used mobile data acess technology to penetrate the wireless network at a Marshalls discount clothing store in St. Paul, Minnesota. They were able to decode data transmitted wirelessly between handheld price-checking devices, cash registers, and the store's computers, and the captured data helped them hack into the central TJX database, which stored customer transactions for T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright stores in the United States and Puerto Rico, and for Winners and HomeSense stores in Canada.

TJX was still using the old Wired Equivalent Privacy (WEP) encryption system, which is relatively easy for hackers to crack. Other companies had switched to the more secure Wi-Fi Protected Access (WPA) standard with more complex encryption, but TJX did not make the change. An auditor later found that TJX had also neglected to install firewalls and data encryption on many of the computers using the wireless network, and didn't properly install another layer of security software it had purchased.

After the hackers tapped into the data transmitted by handheld equipment for communicating price markdowns and checking inventory, they used the data to crack encryption codes so they could digitally eavesdrop on employees logging into TJX's central database in Framingham. They stole one or more user names and passwords and used that information to set up their own accounts in the TJX system, amassing transaction data, including credit card numbers, into about 100 large files. They were able to access the TJX system from any computer connected to the Internet. Company

investigators believe the hackers may have even stolen bank debit card information as customers making purchases waited for their transactions to be approved. TJX acknowledged in a Securities and Exchange Commission filing that it transmitted such data to banks without encryption, violating credit card company guidelines.

A little over a week after discovering the data breach, TJX began to notify the credit card, debit card, and check-processing companies it used that the intrusion had taken place. TJX finally reported the breach to the public in mid-January 2007.

The hackers sold the purloined data on the Internet on password-protected sites used by gangs who run up charges using fake credit cards printed with stolen numbers. Incidents of credit card fraud tied to TJX stores surfaced in the United States and abroad. Customers at Fidelity Homestead, the Louisiana savings bank, began seeing strange transactions on their credit card bills in November 2005—unauthorized purchases in Wal-Mart stores in Mexico and in supermarkets and other stores in southern California.

In March 2007, the Gainesville Police Department and the Florida Department of Law Enforcement arrested six people using fake credit cards with the stolen TJX data. They had purchased $8 million in gift cards from Wal-Mart and Sam's Club stores in 50 Florida counties, and used them to buy flat-screen TVs, computers, and other electronics.

The following July, the U.S. Secret Service arrested four more people in south Florida who had been using the stolen TJX customer data. The suspects were charged with belonging to an organized fraud ring that engaged in identity theft and counterfeit credit card trafficking. The arrests recovered about 200,000 stolen credit card numbers used in fraud losses calculated to be more than $75 million. The fraudsters had purchased the stolen credit card account numbers from known cybercriminals in Eastern Europe.

The revelation quickly directed attention to the way in which the company handled its customers' financial data. In question was whether TJX was adhering to the security rules established by Visa and MasterCard for storing such data, known as the Payment Card Industry (PCI) Data Security Standard. According to these rules, merchants are not supposed to maintain certain types of cardholder data in their systems because the data facilitate the creation of fraudulent card accounts. Communications between Visa and card-issuing financial institutions revealed that TJX did violate this principle by holding onto data for years, rather than for the short amount of time they are actually needed.

Avivah Litan, research director for the Gartner consulting firm, suggested that TJX did not store the data intentionally. Instead, legacy systems that were implemented before hackers were a serious threat accounted for the security catastrophe. Complying with the PCI regulations and fortifying security do not provide a clear return on investment.

TJX was guilty of storing data from Track 2 of the magnetic strip on Visa cards. This area of the strip houses the account number, expiration date, and security code. It does not include names and addresses, which are stored on Track 1. Even though the thieves could not use the data for identity theft, the Track 2 data are sufficient for fabricating false credit cards.

Although the PCI standards are rigorous, merchants who fail to abide by them remain eligible to process electronic payments. The merchant banks who provide the financial network and card readers that let stores accept credit and debit card purchases are subject to fines from Visa of up to $500,000 for accepting transactions from merchants who do not follow PCI rules. In addition to the requirements for storing sensitive data, PCI mandates secure networks with firewalls; systems passwords that are different than the vendor defaults; encryption of sensitive data that crosses public networks, such as the Internet; and up-to-date antivirus software.

TJX responded to the intrusion by launching an investigation with the assistance of a computer security firm. The company advised customers to monitor their accounts for fraudulent activities and established help centers available by a toll-free number and online. The FBI and local authorities, including the Massachusetts Attorney General, also began investigations. In addition to capturing data from the TJX systems, the hacker had covered his tracks by deleting and altering log files, changing clock settings, and relocating data. This made it more difficult to determine which records were accessed and when. In fact, in its 10-K filing to the SEC, TJX admitted that it might never identify much of the stolen data.

Banks that issue credit and debit cards have so far borne the brunt of the TJX losses from fraudulent credit card charges rather than the retailers who accepted the fraudulent cards, the credit card networks such as MasterCard and Visa, or TJX itself. They may have to spend $300 million just to replace the stolen cards, in addition to covering fraudulent purchases. However, lobbyists for banking associations are pushing for laws to place full financial responsibility for any credit card fraud-related losses on the company that allowed its security system to be breached.

Consumer groups and banks have filed lawsuits against TJX and its merchant banks for failing to protect account data. Lawsuits were also filed in six Canadian provinces seeking compensation on behalf of all citizens who might be affected by personal information stolen from TJX stores. According to attorney Archie Lamb, whose firm is among those representing consumers and

banks in their suits against TJX, "the costs to customers and banks will be enormous."

Even without lawsuit liabilities, Forrester Research estimates that the cost to TJX for the data breach could surpass $1 billion over five years, including costs for consultants, security upgrades, attorney fees, and additional marketing to reassure customers. TJX declined to comment on those numbers.

A report from Javelin Strategy & Research revealed that more than 75 percent of the consumers it surveyed would not continue to shop at stores that had been victimized by data theft. The same study showed that consumers trust credit card companies to protect their data far more than retailers. TJX was waiting to discover how much impact its security breach would have on the bottom line.

Sources: Robin Sidel, "Giant Retailer Reveals Customer Data Breach," *The Wall Street Journal,* January 18, 2007; Larry Greenemeier, "Data Theft, Pushback, and the TJX Effect," *InformationWeek*, August 13, 2007; "Secret Service Busts Four Fraudsters with Ties to T.J. Maxx Attack," *InformationWeek*, July 12, 2007, "Hack Attack Means Headaches for TJ Maxx," *Information Week*, February 3, 2007, and T.J. Maxx Probe Reveals Data Brach Worse Than Originally Thought," *InformationWeek*, February 21, 2007; Sharon Gaudin, "Mass. AG Heads Investigation into T.J. Maxx Security Breach, *InformationWeek*, February 9, 2007.

Case Study Questions

1. List and describe the security controls and weaknesses at TJX Companies.
2. What people, organization, and technology factors contributed to these weaknesses?
3. What was the business impact of TJX's data loss on TJX, consumers, and banks?
4. How effectively did TJX deal with these problems?
5. Who should be held liable for the losses caused by the use of fraudulent credit cards in this case? TJX? The banks issuing the credit cards? The consumers? Justify your answer.
6. What solutions would you suggest to prevent the problems?