

## CHAPTER 8

---

# Securing Information Systems

### LEARNING OBJECTIVES

After reading 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?

### OPENING CASE: CANADIAN LAW FIRM WINS THE CASE FOR E-MAIL SECURITY

The opening case draws attention to the inherent issues of email and security, and the differences in jurisdictional legal issues related to the storage of the email. The law firm recognized the responsibility to keep client data and email secure.

As firms become more technologically oriented, they must become more aware of **security** and control issues surrounding their information systems and protect the resources more stringently than ever before.

#### **8.1** **SYSTEM VULNERABILITY AND ABUSE**

---

As our society and the world around us have come to depend on computers and information systems more and more, firms must put forth a better effort in making their systems less vulnerable and more reliable. The systems must also be more secure when processing transactions and maintaining data. These two issues, which we address in this chapter, are the biggest issues facing those wanting to do business on or expand their operations to the Internet. The threats are real, but so are the solutions.

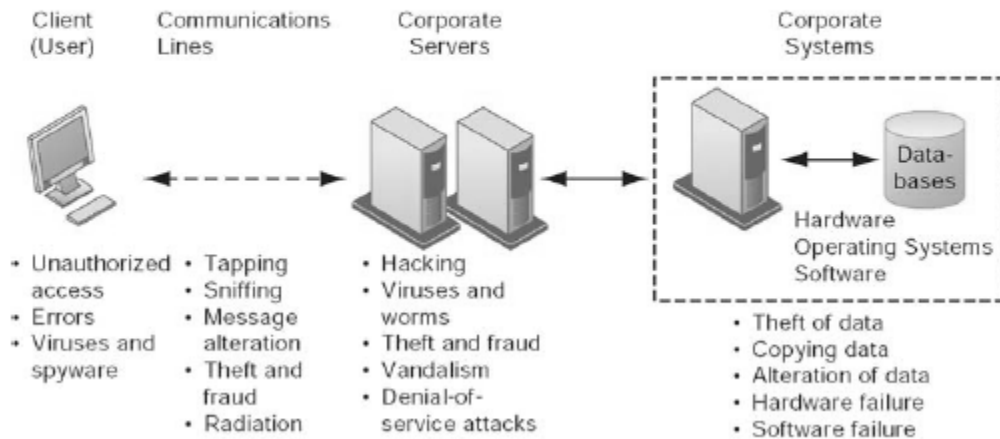
What exactly do we mean when we say that as a business, we need to make security and control a top priority? **Security** refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information

systems. **Controls** consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of accounting records; and operational adherence to management standards.

## WHY SYSTEMS ARE VULNERABLE

Information systems are vulnerable to technical, organizational, and environmental threats from internal and external sources. The weakest link in the chain is poor system management. If managers at all levels don't make security and reliability their number one priority, then the threats to an information system can easily become real. The figure below gives you an idea of some of the threats to each component of a typical network.

**FIGURE 8-1 CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES**



### Internet Vulnerabilities

With distributed computing used extensively in network systems, there are more points of entry into the system. The more people you have using the system, the more potential for fraud and abuse of the information maintained in that system. That's why it is everybody's business to protect the system. It's easy for people to say that they are only one person and therefore they won't make much difference. But it only takes one person to disable a system or destroy data.

You can provide students with current examples of internet vulnerabilities such as hackers stealing corporate or financial data, or employees inadvertently or intentionally transmitting sensitive corporate data to unauthorized parties.

### Wireless Security Challenges

It's a difficult balancing act when it comes to making wireless systems easy to access and yet difficult to penetrate. Internet cafes, airports, hotels, and other hotspot access points

need to make it easy for users to use the network systems with the 802.11 standard. Yet, because it is so easy, hackers and crackers can easily access unsuspecting users' systems and steal data or use the entry point as a way to spread malicious programs. The hackers can use **war driving** techniques to gain access to wireless networks not only in hotels and airports, but private businesses and government centres.

## **WINDOW ON ORGANIZATIONS: DATA THEFT HITS CANADA**

### **TO THINK ABOUT QUESTIONS**

**1. List and describe the potential security control weaknesses at Bell Canada and at C-W Group.**

#### **Security control weaknesses at Bell included:**

- Data stored on unencrypted storage devices
- Storage devices were not secured
- No control over access (passwords)

Security control weaknesses at C-W Group included:

- No control over employee access
- Did not address problem of disgruntled employee
- Decryption code available to employees

**2. What management, organization, and technology factors contributed to these weaknesses?**

**All three elements of an effective technology infrastructure failed in this case.**

**Management:** The main management issue was at C-W Group, where management did not address warning signs that the employee was a potential hazard to security of customer data

**Organization:** There should be separation of duties, so that the same person who can access the data does not have access to the decryption code.

**The organization should have a policy for data storage (encryption for mobile devices).**

**Technology:** There was no encryption of data at Bell. All data was

**stored on the same devices at both organizations (financial and personal data should be stored separately).**

**3. What was the business impact of data loss on these companies and their consumers?**

**The companies spent huge amounts of money investigating and repairing the security compromises on its system. They also suffered from a loss of goodwill with their customers. Defending itself against lawsuits resulting from the data theft will cost it millions of dollars in legal fees and lost income**

**Consumers whose data was stolen may have been compromised because of perceived infringements of privacy, or real instances of identity theft and financial loss.**

**4. Can you tell how effectively each company dealt with these problems?**

**C-W Group took precautions to physically secure their site. Other than that, it is difficult to see what they have done that shouldn't have been done before.**

**5. Who should be held liable for the losses caused by the use of customer credit card information at C-W Group: C-W Group or its customers? Justify your answer.**

**Right now, the credit cards are liable. 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.**

**Student answers will vary.**

**6. What solutions would you suggest to prevent the problems?**

**Student answers will vary. They should address security components such as installing security software on all network access points, wireless networks, and handheld devices. Upgraded wireless security software should be installed and kept current. The company should make security the highest priority. People need to be trained on security issues. They need to establish information system controls and then use them.**

## MIS IN ACTION QUESTIONS

Explore the Web site of the Privacy Commissioner of Canada ([www.priv.gc.ca](http://www.priv.gc.ca)) and review the section on Data Breaches and guidelines for responding to breaches of data security.

1. Based on the details in this case study, how well were Bell and C-W Group complying with these guidelines? What guidelines did they fail to meet?

Much of the information can be found at

[http://www.priv.gc.ca/information/guide/2007/gl\\_070801\\_checklist\\_e.cfm](http://www.priv.gc.ca/information/guide/2007/gl_070801_checklist_e.cfm)

The site provides more information on what to do when a breach occurs, rather than how to prevent it. However, information is added all the time, such as a recent paper describing whether or not businesses needed the driver's license as an i.d.

2. Would complying with these guidelines help to prevent the theft of customer data in the future?

If the data were not collected, then the risk would be lessened. However, the website really deals with response rather than prevention. Each company should have its own security policy to protect both employee and customer data.

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

You can ask students if they have ever picked up a cold or the flu from another human. They probably have, and then it spreads to two or three other people through touch or association. Those people spread it to two or three more people each. Pretty soon it seems that everyone on campus is sick. That is how **computer viruses** are spread. You copy a file from an infected source, use the file, and maybe send it to friends or associates. The virus is now on your computer and spreads to files other than the original. You then send the same or even a different file to a few friends and their computers are infected.

A different type of **malware** called **worms** can also destroy data on computers or clog network systems with software-generated electronic transmissions. Worms are similar to viruses in that they can create additional file copies on a computer and generate e-mails to other computers with the infected file attached. Worms differ from viruses because they don't need human intervention to spread from one computer to another.

**Trojan horses** cause problems because they force a computer system to perform unexpected operations, often to the detriment of the system and the user. This type of malware is usually masked in e-mail messages although it can be stored on Web sites.

Not all **spyware** is damaging to a computer system. It is a popular method for some Web sites to monitor how users navigate through a site, providing critical information that the Web designers and developers can use to improve the site. Unfortunately, some spyware is becoming a popular way for hackers to install malicious code on computers and allows hackers to infiltrate the unsuspecting computer.

**Key loggers** record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers.

Whether you use a stand-alone PC or your computer is attached to a network, you're just asking for trouble if you don't have **antivirus software**. This type of software checks every incoming file for viruses. Not if, but *when*, you receive an infected file, the software alerts you to its presence. You can choose to delete the file or "clean" it. Make sure you update your antivirus software every 30 to 60 days, because new viruses are constantly being written and passed around. Some antivirus software companies now make it very easy to keep your antivirus software current through online updates. McAfee.com and Pandasoftware.com will detect when you are online and notify you when new updates are available. With a few mouse clicks, you download the software to protect against the newest viruses.

Web-enabled and e-mail-enabled cell phones are now being targeted as a way to spread viruses.

## HACKERS AND CYBERVANDALISM

**Hackers**, those who intentionally create havoc or do damage to a computer system, have been around for a long time. Many companies don't report hackers' attempts to enter their systems because they don't want people to realize their systems are vulnerable. That makes gathering real statistics about hacking attempts and successes hard. Unauthorized access is a huge problem, though.

Some hackers penetrate systems just to see if they can. They use special computer systems that continually check for password files that can be copied. Or they look for areas of the system that have been "left open," so to speak, where they can enter the system. Sometimes they don't do any damage, but far too often they destroy files, erase data, or steal data for their own use through the use of Trojan horse software. Other hackers attack systems because they don't like the company. On the other hand, a **cracker** is typically used to describe a hacker who penetrates systems with the sole purpose of criminal intent.

Password theft is the easiest way for hackers to gain access to a system. They generally use specially written software programs that can build various passwords to see if any of them will work. That's why students should use odd combinations of letters and numbers

not easily associated with your name to create your password. The longer the password, the harder it is to replicate.

**Cyber vandalism** is the intentional disruption, defacement, or even destruction of a Web site or corporate information system. Even NASA has not been exempt from the “creative” work of cybervandals.

### **Spoofing and Sniffing**

These are two other methods hackers and criminals can use to gain improper or illegal access to computer systems. **Spoofing** is becoming a common way to steal financial information through fake Web sites. The spoofed site is almost a mirror image of the real site and unless the unsuspecting user examines the spoof closely, he/she may inadvertently give out important personal and financial information.

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. Sniffing is a popular way to “grab” information as it passes over transmission lines whether they are hard-wired or wireless. It is almost impossible to detect and encryption is about the only way to safeguard against it.

### **Denial-of Service-Attacks**

As companies and organizations expand their business to Web sites, they are opening another point of vulnerability through **denial-of-service attacks**. And it seems no Web site is safe: “Hackers attacked the White House Web site Friday, resulting in massive slowdowns, said the Bush administration and a company that monitors the Internet.” The perpetrators sent an enormous amount of data toward the White House site, leaving it completely blocked or difficult to access for about six hours. The White House said no information on the site was altered or destroyed. The connection between the White House’s Internet service provider and [www.whitehouse.gov](http://www.whitehouse.gov) became clogged with data in what is commonly called a “denial of service attack,” said Jimmy Orr of the White House media affairs office. (*USA Today*, May 7, 2001)

A **distributed denial-of-service (DDoS)** attack uses hundreds or even thousands of computers to inundate and overwhelm the network from numerous launch points. Although DoS attacks are not designed to destroy information or access restricted areas of a company’s information system, they can create havoc due to the fact that they can literally shut down the system which results in lost productivity and business.

DoS attackers often utilize thousands of “zombie” computers to launch their DoS attacks. Once infected with malicious software, these computers create a **botnet** where the infected computers are controlled by the actions of the hacker.

## **COMPUTER CRIME AND CYBERTERRORISM**

Computer crime is a growing national and international threat to the continued development of e-business and e-commerce. When the Internet was first created in the

late 1960s, the designers intentionally built it to be open and easily accessible. Little did they know that 40 years later, that structure would be the very cause of so much crime and vandalism. Table 8-2 lists the best known examples of computer crime.

**TABLE 8-2 EXAMPLES OF COMPUTER CRIME**

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

### Identity Theft

“The fastest growing crime off or on the Internet is **identity theft**. Even though identity theft is most likely to occur in an offline environment, once your personal information has been stolen its easy to use it in an online environment. The biggest risk for identity fraud is from the old-fashioned theft of your wallet or paper records from your trash. And from people who know you. People who are close to you can set up known accounts and have the information sent to a new address. So the fraud goes on longer and is harder to discover,” says James Van Dyke of Javelin Strategy in Pleasanton, California. (*USA Today Online*, Jan 26, 2005)

There are many precautions an online user can take to help prevent identity theft. One way is to scrutinize e-mails or phone calls that ask for your personal information or financial account information. No legitimate financial institution will ever send an e-mail requesting you to supply your account information. That is the number one indicator that the e-mail is a **phishing** e-mail. You should ignore and delete the e-mail immediately. You can also request free credit reports from the three major credit bureaus once a year to monitor the information about your credit card and financial activities.

Two new phishing techniques called evil twins and pharming. By definition, **evil twins** are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet. The bogus network looks identical to a legitimate public network. **Pharming** redirects users to a bogus Web page, even when the individual types the correct Web page address into their browser.

### Click Fraud



We are all familiar with unwanted advertisement ads displaying on our monitors. However, did you know that every time 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? Who would have thought that this annoying practice is actually a big problem? Well — it is. Some experts believe that it is the single largest threat to search engine marketing. **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.

### **Cyberterrorism and Cyberwarfare**

As terrorism continues to increase the possibility of physical attacks anywhere in the world, computer systems can be targeted as often as buildings, cars, or trains. Governments realize this and are investigating ways of preventing system attacks or minimizing the damage caused to the vast number of networks that are vulnerable.

## **INTERNAL THREATS: EMPLOYEES**

Students are often surprised to learn that most computer crime against companies is committed by current or former employees, those who know the system best, are entrusted with huge amounts of data, and have the easiest access. Managers and executives need to be aware of potential internal threats to their systems and put special measures in place to safeguard systems and data. They also need to impress upon all employees how important security is throughout the system right down to the last person.

Safeguarding individual passwords from **social engineering** maliciousness is the responsibility of everyone in the organization. An effective way of limiting access to data is to establish computer-generated logs that show every employee who logged on, what they did, what part of the system they accessed, and whether any data were used or updated. Logs are easily created by system software programs and should be periodically reviewed by the information technology staff and department managers. If nothing else, it gives them an idea of what their employees are doing.

## **SOFTWARE VULNERABILITY**

The term bug, used to describe a defect in a software program, has been around since the 1940s and 1950s. Back then, computers were powered by vacuum tubes — hundreds and thousands of them. Grace Hopper, an early computer pioneer, was troubleshooting a computer that had quit running. When her team opened the back of the computer to see what was wrong, they found a moth had landed on one of the tubes and burnt it out. She coined the term “bug” to describe a problem with computers.

With millions of lines of code, it's impossible to have a completely error-free program. Most software manufacturers know their products contain bugs when they release them to the marketplace. They provide free updates, patches, and fixes on their Web sites. That's why it's a good idea not to buy the original version of a new software program but to wait until some of the major bugs have been found and corrected.

Because bugs are so easy to create, most unintentionally, you can reduce the number of them in your programs by using the tools discussed in other chapters to design good programs. Many bugs originate in poorly defined and designed programs and keep infiltrating all parts of the program.

Most software users are familiar with the concept of software patches. **Patches** are released by software manufacturers in order to repair flaws. These small pieces of software are easily installed and do not disturb the proper operation of the software. An excellent example of software patches has been evident in the Microsoft operating systems and the office product packages.

**Bottom Line: Information systems security is everyone's business. Use antivirus software on your computer and update it often. The "it won't happen to me" attitude is trouble. Instituting measures to decrease the bugs and defects in software and data entry can solve many system quality problems.**

## 8.2

## BUSINESS VALUE OF SECURITY AND CONTROL

Emphasize that transactions worth billions and trillions of dollars are carried out on networks every day, and ask students to think of the impact if the networks experience downtime for even a few minutes.

In 2005 ChoicePoint, a data brokerage company, revealed that they had inadvertently sold personal and financial information to more than 50 companies that were fronts for identity thieves. This incident underscores the difficulties with protecting data and information on millions of unsuspecting consumers and legitimate businesses. The problem of how to protect the data may very well be decided by the courts.

Recent examples include TJMax, which reported that a breach of their system had allowed customer data, including credit card and debit card information, to be compromised.

## LEGAL AND REGULATORY REQUIREMENTS FOR ELECTRONIC RECORDS MANAGEMENT

Because so much of our personal and financial information is now maintained electronically, the Canadian government is beginning to pass laws (PIPEDA in Chapter 4, and CSOX) mandating how the data will be protected from unauthorized or illegal misuse. Firms face new legal obligations for electronic records management and document retention as well as for privacy protection. **Electronic records management**

**(ERM)** consists of policies, procedures, and tools for managing the retention, destruction, and storage of electronic records. ERM is a key item in CSOX (Canadian Rules for Sarbanes-Oxley Act), which protects investors from fraudulent corporate practices.

## ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

Several things are happening in the corporate world that are changing the requirements for how companies handle their electronic documents: 1) Companies are communicating more and more with e-mail and other forms of electronic transmissions, and 2) Courts are allowing all forms of communication to be held as evidence. Therefore businesses must develop methods of capturing, storing, and presenting any and all electronic communications including e-mail, instant messaging, and e-commerce transactions.

**Computer forensics** is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media.

**Bottom Line: Regardless of where or how electronic transmissions were generated or received, businesses are now responsible for making sure they are monitored, stored, and available for scrutiny. These new requirements significantly change the way businesses view their information resources.**

### 8.3

## ESTABLISHING A FRAMEWORK FOR SECURITY AND CONTROL

Students should understand how you can prevent some of the problems discussed? One of the best ways is to institute **controls** in an information system the same way one might in any other system; through methods, policies, and procedures.

Ask students to think about what a typical company does when it builds a new office building. From the beginning of the design phase until the building is occupied, the company decides how the physical security of the building and its occupants will be handled. It builds locks into the doors, maybe even designs a single entry control point. It builds a special wing for the executive offices that perhaps might have extra thick bulletproof glass. There are fences around the perimeter of the building that control the loading docks.

These are just a few examples to get students to think about the fact that the company designs the security into the building from the beginning. It doesn't wait until everything is built. You should do the same thing with an information system. It's no different from any other system that requires planning and well-thought-out policies and procedures *before* construction begins.

**ISO 17799** is an international set of standards for security and control, provides helpful guidelines. It specifies best practices in information systems security and control, including security policy, business continuity planning, physical security, access control, compliance, and creating a security function within an organization.

## RISK ASSESSMENT

Companies and government systems constantly use **risk assessment** to determine weak links in their physical building security. Tell students that the same methodology can be used to assess the risk in your information system. Use risk assessment to set up cost comparisons for developing and maintaining security against the loss potential.

## SECURITY POLICY

Companies spend a lot of money on physical security such as locks on doors or fences around supply depots. They need to do the same thing for their information systems. Because of the increasing liability for security breaches, many companies are now establishing a **chief security officer** position to help ensure the firm maximizes the protection of information resources. Some tools available to the CSO are:

- **Security policy:** principle document that determines security goals and how they will be achieved
- **Acceptable use policy (AUP):** outlines acceptable and unacceptable uses of hardware and telecommunications equipment
- **Authorization policy:** determines what access users may have to information resources
- **Authorization management systems:** manages access to each part of the information system.

Figure 8-4 shows how the authorization management system would limit access for two different users.

**FIGURE 8-4 SECURITY PROFILES FOR A PERSONNEL SYSTEM**

SECURITY PROFILE 1	
User: Personnel Dept. Clerk	
Location: Division 1	
Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116	
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2	
User: Divisional Personnel Manager	
Location: Division 1	
Employee Identification Codes with This Profile: 27321	
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

## DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Many companies create **fault-tolerant computer systems** that are used as back-ups to help keep operations running if the main system should go out. These back-up systems add to the overall cost of the system — but think about the losses if the system experiences a significant period of downtime. Add the cost of lost productivity by employees to lost transactions and unhappy customers; you do the math. Just imagine what would happen if an airline reservation system (a typical **online transaction processing** system) went down. Have you ever called a company to place an order for a new dress and it couldn't take your order because the computer was down? Maybe you called back later, and maybe you didn't.

Make sure students understand the difference between fault-tolerant computer systems and **high-availability computing**:

- Fault-tolerant computer systems promise continuous availability and eliminate recovery time altogether.
- High-availability computer systems help firms recover quickly from a crash.

High-availability computer systems use the following tools to ensure digital firms have continuous computing capacity available:

- load balancing

- redundant servers
- mirroring
- clustering
- storage area networks
- disaster recovery plan
- recovery-oriented computing

Perhaps the most important element of a successful system is **disaster recovery planning**. Firms around the world discovered the necessity for a well-written and tested disaster recovery plan on September 11, 2001. Those firms that had completed **business continuity planning** were able to carry on business, while those that hadn't, spent days and weeks recovering from the terrorist attacks.

### Security Outsourcing

If your company lacks the internal resources to adequately plan for disaster, you can use an outside source such as **managed security service providers**. They may be better at the necessary planning and offering appropriate hardware and software resources because they specialize in such things.

## THE ROLE OF AUDITING

Companies audit their financial data using outside firms to make sure there aren't any discrepancies in their accounting processes. Perhaps they audit their supply systems on a periodic basis to make sure everything is on the up-and-up. They should also audit their information systems. After all, information is as an important resource as any other in the organization. **MIS audits** verify that the system was developed according to specifications, that the input, processing, and output systems are operating according to requirements, and that the data is protected against theft, abuse, and misuse. In essence, an MIS audit checks all the controls we've discussed in this chapter.

**Bottom Line: Controls, general and application, must be designed into the system at the beginning, not as an afterthought. General controls are concerned with the system software and manual procedures. Application controls protect the data input, the data processing, and the information output. The tools available for ensuring business continuity include fault-tolerant systems and high-availability computing. Business continuity and disaster recovery planning are more important than ever for businesses.**

**8.4****TECHNOLOGIES AND TOOLS FOR SAFEGUARDING INFORMATION RESOURCES**

---

An array of tools and technologies are available to secure systems and data. They include tools for authentication, firewalls, intrusion detection systems, antivirus and antispyware software, and encryption. Show students some of the ways a firm can help protect itself.

**ACCESS CONTROL**

The headlines telling of hackers' exploits in the past year should be enough to convince every company of the need to install firewalls, **access controls**, and other security measures. With the installation of cable modems or DSL lines, home users must follow the same guidelines. These new connections, which leave your personal computer "always on," are just as vulnerable to attacks as corporate systems.

In corporate systems, it's important to ensure **authentication** methods are in place so that unauthorized users can't gain access to the system and its data. Because most simple password systems are too weak and make the system too vulnerable, security experts are devising new methods to control access.

Newer authentication technologies, such as tokens, smart cards, and biometric authentication are being used as means for more elaborate access control. A **token** is a physical device that is designed to prove the identity of a single user. A **smart card** is a device that contains a chip formatted with access permission and other data.

**Biometric authentication** is becoming more popular as a method of protecting systems and data as the technology is refined. Although you may have seen the fingerprint or facial recognition techniques only on sci-fi movies, rest assured it may be the next wave of security that's installed in your organization.

If you allow employees to keep certain data on their machines that are not backed up to the mainframe computer, you need to ensure that safeguards are installed on the individual PCs. Make sure you have controls in place for access to individual data, backing it up, and properly protecting it against corruption. Do you even have a policy about whether employees can store data on their individual terminals?

**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**

The four types of firewalls described in the text are:

- **Packet filtering:** data packet header information is examined in isolation
- **Network address translation (NAT):** conceals IP addresses and makes it more difficult to penetrate systems
- **Application proxy filter:** sort of like a fence through which a substitute message passes.
- **Stateful inspection:** the actual message comes through the firewall but must be identified by the user as passable.

### Intrusion Detection Systems

Firewalls can deter, but not completely prevent, network penetration from outsiders and should be viewed as one element in an overall security plan. In addition to firewalls, digital firms relying on networks use **intrusion detection systems** to help them protect their systems.

### Antivirus and Antispyware Software

While most computer users, especially home users, know they are supposed to have **antivirus software** installed, they may be negligent in keeping it up-to-date. Because new viruses are unleashed almost every week, antivirus software needs constant updating — at least once a week. Many brand-name software programs have an automatic update feature that users should take advantage of.

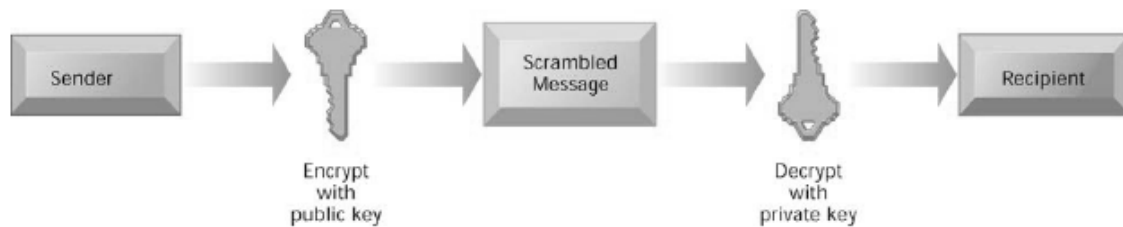
## SECURING WIRELESS NETWORKS

It's becoming more important for Wi-Fi users to protect their data and electronic transmissions as wireless networks and their access points proliferate around the country. Security is easily penetrated because of the very nature of the spectrum transmission used in Wi-Fi. Unless users take stringent precautions to protect their computers, it's relatively easy for hackers to obtain access to files. Stronger encryption and authentications systems for Wi-Fi than the original Wired Equivalent Privacy (WEP) is being installed in newer computer models. But individual users still carry the responsibility to make sure passwords are changed from the original and encryption systems are used to help protect data.

## ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE

Most people are reluctant to buy and sell on the Internet because they're afraid of theft, fraud, and interception of transactions. To help ease the mind and make transactions secure, many companies are using very sophisticated methods of protecting data as they travel across the various transmission media.



**FIGURE 8-7 PUBLIC KEY ENCRYPTION**

This figure shows you how **encryption** works using public and private keys. The keys are created through complicated mathematical formulas. The longer the key, the harder it is to decipher. That's the whole point of encryption.

Encryption software programs incorporate authentication and message integrity in its program to ensure senders and receivers are protected against many of the computer crimes committed on networks and the Internet.

Two methods of encrypting network traffic on the Web are SSL and S-HTTP. **Secure Sockets Layer (SSL)** 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.

Usually you can't tell if a transmission is authentic when you receive it over the Internet or network. **Digital signature** software can create a method of verifying that the message, document, or file has not been altered between the time it left the sender and you received it. The Electronic Signatures in Global and National Commerce Act authorized the use of digital signatures and promises to enhance electronic commerce and make it easier to do business digitally. You must be careful though as digital signatures can be forged or altered the same as an old-fashioned, handwritten signature can be forged.

Another way of providing authenticity to network transmissions is by using a **digital certificate**. Just as your personal signature is connected to you, a digital certificate provides a way of proving you are who you say you are. GlobalSign.com has lots of information about its digital certificate product and other useful information about this technology. You can get a demo certificate, find someone's certificate, or get more information about how to use your own certificate.

Two methods companies are using to make online transactions more secure are Secure Socket Layers and Secure Hypertext Transport Protocol. The next time you're on an e-commerce or e-business Web site, look in the address text box of your browser and notice if the address begins with https:. If so, the site incorporates one of these two security measures. **Public key infrastructure (PKI)** is another method for providing secure

authentication of online identity and makes users more comfortable transacting business over networks.

**Bottom Line: Some of the technologies and tools businesses can use for security and control include access control, firewalls, intrusion detection systems, antivirus software, encryption, and ensuring software reliability. Security is everyone's concern throughout the organization.**

## **WINDOW ON TECHNOLOGY: CAN SALESFORCE.COM ON-DEMAND REMAIN IN DEMAND?**

### **TO THINK ABOUT QUESTIONS**

#### **1. How did the problems experienced by Salesforce.com impact its business?**

Obviously the outages that Salesforce.com experienced prevented it from carrying on normal business routines. The idea behind its business model is to provide on-demand computing services to other businesses at a 99.9 percent rate. Salesforce.com was growing rapidly and seeking to attract more large customers with new software and services in addition to CRM. Because of the outages, convincing enterprise customers to let it run their applications was much more difficult. The first outage didn't necessarily create a crisis a confidence, but the continuing problems did. The company failed to adequately communicate with its customers about the problem causing even more dissatisfaction with the company.

#### **2. How did the problems impact its customers?**

If subscribers to its services can't access their data and applications, then their businesses are impacted. With no access to customers' records, some businesses came to a standstill for the duration of the outages. Every time Salesforce.com had to restart each database instance in a cluster, it had to interrupt service. The company's customers began to distrust the service and turn to other sources for computing services.

#### **3. What steps did Salesforce.com take to solve the problems? Were these steps sufficient?**

Initial steps to solve the problems were not sufficient. The problems were not limited to software bugs as initially thought. The recurring outages raised doubts about the fidelity of the service's infrastructure as a whole. Customers complained about poor customer service and a tepid response from management. Salespeople were described as arrogant and interested only in selling more user licenses. The CEO was criticized for downplaying the interruptions as minor when they were anything but.

The company improved its client communications, updating them on efforts to resolve the service problems. It developed a Web site that displayed both real-time and historical data related to performance measurements of key components. That was important to help soothe customer concerns.

It also invested \$50 million in a mirroring system that creates a duplicate database in a separate location and synchronizes the data instantaneously. It added two data centers on each coast enabling it to distribute processing and balance its database load. Ultimately it strengthened its IT infrastructure to the point where outages were no longer occurring.

**4. List and describe other vulnerabilities discussed in this chapter that might create outages at Salesforce.com and measures to safeguard against them.**

Other vulnerabilities Salesforce.com needs to protect against include:

- Viruses: install and continually update antivirus software
- Authorization and authentication: ensure only authorized users have access to the systems and ensure authentication measures are continually reviewed
- Denial-of-service attacks: install botnet detection software and keep firewalls and antivirus software up to date
- Employees: ensure employees are continually trained on system security and how to identify unauthorized use of the systems and networks

## MIS IN ACTION QUESTIONS

**Go to [www.trust.salesforce.com](http://www.trust.salesforce.com), explore the site, and answer the following questions:**

**1. How does this site help Salesforce.com promote security among its users?**

*Excerpt copied directly from Salesforce.com Web site:*

"Salesforce.com utilizes some of the most advanced technology for Internet security available today. When you access our site using Netscape Navigator 6.0 or Microsoft Internet Explorer versions 5.5 or higher, Secure Socket Layer (SSL) technology protects your information using both server authentication and data encryption, ensuring that your data is safe, secure, and available only to registered Users in your organization. Your data will be completely inaccessible to your competitors.

Salesforce.com provides each User in your organization with a unique user name and password that must be entered each time a User logs on. Salesforce.com issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user. Salesforce.com does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

In addition, salesforce.com is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders."

**2. If you ran a business, would you feel confident about using Salesforce.com's on-demand service? Why or why not?**

Answers will vary but should address security components as well as a comparison to other services available, including in-house computing capacity.

## **SUMMARY**

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

With data concentrated into electronic form and many procedures invisible through automation, computerized information systems are vulnerable to destruction, misuse, error, fraud, and hardware or software failures. Corporate systems using the Internet are especially vulnerable because 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 disruptions. Wi-Fi networks easily can be penetrated by intruders using sniffer programs to obtain an address to access the resources of the network. Computer viruses and worms can spread rampantly from system to system, clogging computer memory or destroying programs and data. 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 can introduce errors.

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

Security and control are important but often neglected areas for information systems investments. Firms relying on computer systems for their core business functions can 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 an appropriate organizational and managerial framework for security and control to use technologies effectively to protect their information resources. 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. A disaster recovery plan provides procedures and facilities for restoring computing and communications services after they have been disrupted, whereas a business continuity plan focuses on how the company can restore business operations.

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?***

Companies require special measures to support electronic commerce and digital business processes. They can use fault-tolerant computer systems or create high-availability computing environments to make sure that their information systems are always available and performing without interruptions. Firewalls are placed between an organization's private network and external networks, such as the Internet, to prevent unauthorized users from accessing the private network. 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 the Internet and over Wi-Fi networks. Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user's identity.

## KEY TERMS

The following alphabetical list identifies the key terms discussed in this chapter.

***Acceptable use policy*** — defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet, and specifies consequences for noncompliance.

***Access control*** — policies and procedures a company uses to prevent improper access to systems by unauthorized insiders and outsiders.

***Antivirus software*** — software designed to detect, and often eliminate, computer viruses from an information system.

***Application proxy filtering*** — firewall screening technology that uses a proxy server to inspect and transmit data packets flowing into and out of the organization so that all the

organization's internal applications communicate with the outside using a proxy application.

**Authentication** — the ability of each party in a transaction to ascertain the identity of the other party.

**Authorization management systems** — systems for allowing each user access only to those portions of a system or the Web that person is permitted to enter, based on information established by a set of access rules.

**Authorization policies** — policies that determine differing levels of access to information assets for different levels of users in an organization.

**Biometric authentication** — technology for authenticating system users that compares a person's unique characteristics, such as fingerprints, face, or retinal image, against a stored set profile of these characteristics.

**Botnet** — a group of computers that have been infected with bot malware without users' knowledge, enabling a hacker to use the amassed resources of the computers to launch distributed denial-of-service attacks, phishing campaigns, or spam.

**Business continuity planning** — planning that focuses on how the company can restore business operations after a disaster strikes.

**Chief security officer (CSO)** — heads a formal security function for the organization and is responsible for enforcing the firm's security policy.

**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.

**Computer forensics** — 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.

**Computer virus** — rogue software program that attaches itself to other software programs or data files in order to be executed, often causing hardware and software malfunctions.

**Controls** — all the methods, policies, and procedures that ensure protection of the organization's assets, accuracy and reliability of its records, and operational adherence to management standards.

**Cracker** — a hacker with criminal intent.

**Cyber vandalism** — intentional disruption, defacement, or even destruction of a Web site or corporate information system.

**Denial-of-service (DoS) attack** — flooding a network server or Web server with false communications or requests for services in order to crash the network.

**Digital certificates** — attachments to an electronic message to verify the identity of the sender and to provide the receiver with the means to encode a reply.

**Digital signature** — a digital code that can be attached to an electronically transmitted message to uniquely identify its contents and the sender.

**Disaster recovery planning** — planning for the restoration of computing and communications services after they have been disrupted.

**Distributed denial-of-service (DDoS) attack** — numerous computers inundate and overwhelm a network from numerous launch points.

**Downtime** — period of time in which an information system is not operational.

**Electronic records management (ERM)** — policies, procedures, and tools for managing the retention, destruction, and storage of electronic records.

**Encryption** — the coding and scrambling of messages to prevent their being read or accessed without authorization.

**Evil twin** — wireless networks that pretend to be legitimate Wi-Fi networks to entice participants to log on and reveal passwords or credit card numbers.

**Fault-tolerant computer systems** — systems that contain extra hardware, software, and power supply components that can back a system up and keep it running to prevent system failure.

**Gramm-Leach-Bliley Act** — law that requires financial institutions to ensure the security and confidentiality of customer data.

**Hacker** — a person who gains unauthorized access to a computer network for profit, criminal mischief, or personal pleasure.

**High-availability computing** — tools and technologies, including back-up hardware resources, to enable a system to recover quickly from a crash.

**HIPAA** — law outlining 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.

**Identity theft** — theft of key pieces of personal information, such as credit card or social security numbers, in order to obtain merchandise and services in the name of the victim or to obtain false credentials.

**Intrusion detection systems** — tools to monitor the most vulnerable points in a network to detect and deter unauthorized intruders.

**ISO 17799** — an international set of standards for security and control of information services.

**Key loggers** — spyware that records every keystroke made on a computer.

**Malware** — malicious software programs, such as computer viruses, worms, and Trojan horses.

**Managed security service providers (MSSPs)** — companies that provide security management services for subscribing clients.

**MIS audit** — identifies all the controls that govern individual information systems and assess their effectiveness.

**Network address translation (NAT)** — conceals the IP address 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.

**Online transaction processing** — transaction processing mode in which transactions entered online are immediately processed by the computer.

**Packet filtering** — examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet.

**Patches** — small pieces of software that repair flaws in programs without disturbing the proper operation of the software.

**Pharming** — phishing technique that redirects users to a bogus Web page, even when the individual types the correct Web page address into his or her browser.

**Phishing** — a form of spoofing involving setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data.

**Public key infrastructure (PKI)** — system for creating public and private keys using a certificate authority (CA) and digital certificates for authentication.

**Recovery-oriented computing** — computer system designed to recover rapidly when mishaps occur.



**Risk assessment** — determining the potential frequency of the occurrence of a problem and the potential damage if the problem were to occur. Used to determine the cost/benefit of a control.

**Sarbanes-Oxley Act** — law passed in 2002 that imposes responsibility on companies and their management to protect investors by safeguarding the accuracy and integrity of financial information that is used internally and released externally.

**Secure Hypertext Transfer Protocol (S-HTTP)** — protocol used for encrypting data flowing over the Internet; limited to individual messages.

**Secure Sockets Layer (SSL)** — enables client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session.

**Security** — policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

**Security policy** — statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals.

**Smart card** — a credit-card size plastic card that stores digital information and that can be used for electronic payments in place of cash.

**Sniffer** — a type of eavesdropping program that monitors information traveling over a network.

**Social engineering** — tricking people into revealing their passwords by pretending to be legitimate users or members of a company in need of information.

**Spoofing** — misrepresenting one's identity on the Internet or redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.

**Spyware** — technology that aids in gathering information about persons or organizations without their knowledge.

**Stateful inspection** — provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver.

**Token** — physical device, similar to an identification card, that is designed to prove the identity of a single user.

**Transport layer security (TLS)** — successor to SSL, which enables client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session.

**Trojan horse** — a software program that appears legitimate but contains a second hidden function that may cause damage.

**War driving** — an eavesdropping technique in which eavesdroppers drive by buildings or park outside them trying to intercept wireless network traffic.

**Worms** — independent software programs that propagate themselves to disrupt the operation of computer networks or destroy data and other programs.

## REVIEW QUESTIONS

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

List and describe the most common threats against contemporary information systems.

**The most common threats against contemporary information systems include: technical, organizational, and environmental factors compounded by poor management decisions. Figure 8-1 includes the following:**

**Technical: unauthorized access, introducing errors**

**Communications: tapping, sniffing, message alternation, theft and fraud, radiation**

**Corporate servers: hacking, viruses and worms, theft and fraud, vandalism, denial of service attacks**

**Corporate systems: theft of data, copying data, alteration of data, hardware failure, and software failure. Power failures, floods, fires, or other natural disasters can also disrupt computer systems.**

**Poor management decisions: poor safeguard design to protect valuable data from being lost, destroyed, or fall into the wrong hands.**

Define malware and distinguish among a virus, a worm, and a Trojan horse.

**Malware (for malicious software) is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware programs that gather information about a computer user without permission.**

**Virus:** a program or programming code that replicates itself by being copied or initiating its copying to another program, computer boot sector or document.

**Worm:** a self-replicating virus that does not alter files but resides in active memory and duplicates itself without human intervention.

**Trojan horse.** a program in which malicious or harmful code is contained inside apparently harmless programming or data. A 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.

Define a hacker and explain how hackers create security problems and damage systems.

A hacker is an individual who gains unauthorized access to a computer system by finding weaknesses in security protections used by Web sites and computer systems. Hackers not only threaten the security of computer systems, but they also steal goods and information, as well as damage systems and commit cybervandalism. They may intentionally disrupt, deface, or even destroy a Web site or corporate information system.

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.

The Department of Justice defines computer crime as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution.” Computer crime is defined as the commission of illegal acts through the use of a computer or against a computer system. Table 8-2 provides examples of computer crimes.

**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**

**Internationally attempting to intercept electronic communication**

**Illegally accessing stored electronic communications, including e-mail and voice mail**

**Transmitting or processing child pornography using a computer**

Define identity theft and phishing and explain why identity theft is such a big problem today.

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security identification number, driver's license number, 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.

It is a big problem today as the Internet has made it easy for identity thieves to use stolen information because goods can be purchased online without any personal interaction. Credit card files are a major target of Web site hackers. Moreover, e-commerce sites are wonderful sources of customer personal information that criminals can use to establish a new identity and credit for their own purposes.

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 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 or by entering the information at a bogus Web site. New phishing techniques such as evil twins and pharming are very hard to detect.

Describe the security and system reliability problems created by employees.

**The largest financial threats to business institutions come from employees. Some of the largest disruptions to service, destruction of e-commerce sites, and diversion of customer credit data and personal information have come from insiders. 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.**

**Many employees forget their passwords to access computer systems or allow other coworkers 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 (social engineering). Employees can introduce errors by entering faulty data or by not following proper instructions for processing data and using computer equipment. Information specialists can also create software errors as they design and develop new software or maintain existing programs.**

**Explain how software defects affect system reliability and security.**

**The software can fail to perform, perform erratically, or give erroneous results because of undetected bugs. A control system that fails to perform can mean medical equipment that fails or telephones that do not carry messages or allow access to the Internet. A business system that fails means customers are under- or over-billed. Or, it could mean that the business orders more inventory than it needs. Or an automobile's braking system may fail.**

**Major quality problems are the bugs or defects caused by incorrect design. The other problem is maintenance of old programs caused by organizational changes, system design flaws, and software complexity. Bugs in even mildly complex programs can be impossible to find in testing, making them hidden bombs.**

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

**Explain how security and control provide value for businesses.**

**Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to**

**information systems.**

**Controls consist of all the methods, policies, and organizational procedures that ensure the safety of the organization's assets; the accuracy and reliability of its account records; and operational adherence to management standards.**

**Security and control provide business value by:**

**Firms relying on computer systems for their core business functions can 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.**

**Describe the relationship between security and control and recent government regulatory requirements and computer forensics.**

**Legal actions requiring electronic evidence and computer forensics also require firms to pay more attention to security and electronic records management. 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 the 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**

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

**Define general controls and describe each type of general control.**

**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. They apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.**

**Table 8.3 describes each type of general control**

**Define application controls and describe each type of application control.**

**Application controls are specific controls unique to each computerized application. 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:**

**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.**

**Describe the function of risk assessment and explain how it is conducted for information systems.**

**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. Controls can be adjusted or added to focus on the areas of greatest risk. An organization does not want to over-control areas where risk is low and under-control areas where risk is high.**

**Security risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of the firm's risks, and ranking those risks by level of severity. This process involves making cost-effective decisions on what you want to protect. The old security adage says that you should not spend more to protect something than it is actually worth. A full treatment of risk analysis is outside the scope of this section; however, there are two elements of a risk analysis that should be briefly covered for the students: (1) identifying the assets and (2) identifying the threats. For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an**

eye to how the threat could affect these areas. One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious, like all the various pieces of hardware, but some are overlooked, such as the people who actually use the systems. The essential point is to list all things that could be affected by a security problem.

Define and describe the following: security policy, acceptable use policy, authorization policy.

A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. 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 each user and specifies consequences for noncompliance.

Authorization policy determines 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.

Explain how MIS auditing promotes security and control.

Comprehensive and systematic MIS auditing organizations determine the effectiveness of security and controls for their information systems. An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. Control weaknesses and their probability of occurrence will be noted. The results of the audit can be used as guidelines for strengthening controls, if required.



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

**Name and describe three authentication methods.**

**Authentication refers to the ability to know that a person is who he or she claims to be. Some methods are described below:**

**What you know: Passwords known only to the authorized users.**

**What you have:**

**Token is a physical device that is designed to provide the identity of a single user**

**Smart card is a device that contains a chip formatted with access permission and other data.**

**What you are: Biometrics is based on the measurement of a physical or behavioural trait that makes each individual unique.**

**Describe the roles of firewalls, intrusion detection systems, and antivirus software in promoting security.**

**A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. Firewalls prevent unauthorized users from accessing internal networks. They protect internal systems by monitoring packets for the wrong source or destination, or by offering a proxy server with no access to the internal documents and systems, or by restricting the types of messages that get through, for example, e-mail. Further, many authentication controls have been added for Web pages as part of firewalls.**

**Intrusion detection systems monitor the most vulnerable points or “hot spots” in a network to detect and deter unauthorized intruders. These systems often also monitor events as they happen to look for security attacks in progress. Sometimes they can be programmed to shut down a particularly sensitive part of a network if it receives unauthorized traffic.**

**Antivirus software is designed to check computer systems and drives for the presence of computer viruses and worms and often eliminates the malicious software, whereas antispyware software combats intrusive and harmful spyware programs. Often the software can eliminate the virus from the infected area. To be effective, antivirus software must be continually updated.**

**Explain how encryption protects information.**

**Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over the Internet and over Wi-Fi networks. Encryption offers protection by keeping messages or packets hidden from the view of unauthorized readers. Encryption is crucial for ensuring the success of electronic commerce between the organization and its customers and between the organization and its vendors.**

**Describe the role of encryption and digital certificates in a public key infrastructure.**

**Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user's identity. Digital certificates are data fields used to establish the identity of the sender and to provide the receiver with the means to encode a reply. These use a trusted third party known as a certificate authority to validate a user's identity. Both digital signatures and digital certificates play a role in authentication. Authentication refers to the ability of each party to know that the other parties are who they claim to be.**

**Distinguish between fault-tolerant and high-availability computing, and between disaster recovery planning and business continuity planning.**

**Fault-tolerant computer systems contain redundant hardware, software, and power supply components that can back the system up and keep it running to prevent system failure. Some systems simply cannot be allowed to stop, such as stock market systems or some systems in hospitals. Fault-tolerant computers contain extra memory chips, processors, and disk storage devices to backup a system and keep it running to prevent failure. They also can use special software routings or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device.**

**High-availability computing, though also designed to maximize application and system availability, helps firms recover quickly from a crash. 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 requirements or for firms that depend on digital networks for their internal operations.**

**Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack. 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. 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.**

**Describe measures for improving software quality and reliability.**

**Using software metrics and rigorous software testing are two measure for improving software quality and reliability.**

**Software metrics are objective assessments of the system in the form of quantified measurements. Metrics allow an information systems department and end users to jointly measure the performance of a**

**system and identify problems as they occur. Metrics must be carefully designed, formal, objective, and used consistently. Examples of software metrics include:**

**Number of transactions that can be processed in a specified unit of time**

**Online response time**

**Number of known bugs per hundred lines of program code**

**Early, regular, and thorough testing will contribute significantly to system quality. Testing can prove the correctness of work but also uncover errors that always exist in software. Testing can be accomplished through the use of:**

**Walkthroughs: a review of a specification or design document by a small group of people**

**Coding walkthroughs: once developers start writing software, these can be used to review program code.**

**Debugging: when errors are discovered, the source is found and eliminated**

### **Discussion Questions**

**Security isn't simply a technology issue, it is a business issue. Discuss your opinion.**

**Computer systems, of course, are composed of a number of technological marvels. As any asset in an organization, they need to be kept secure. A company's core capabilities and business processes are vital in today's digital world. Technology plays an increasing and vital role in our daily life and firms need to make these systems secure.**

**Securing these systems refer to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to the information systems. On the other hand, technology is not the key issue in information systems security and control. The technology provides a foundation, but in the absence of intelligent management policies, even the best technology can be easily defeated. Protection of information resources requires a sound security policy and set of controls. A business policy specifies best practices in information systems security and control, including security policy, business continuity planning, physical security, access control, compliance, and creating a security function within the organization.**

**Without secure systems, no business will function for very long.**

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

**Business managers and information technology specialists need to work together 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.**

**Students should be encouraged to search the Internet for examples of business continuity plans. An example of what topics need to be covered in developing a business continuity plan can be found at the following Web site: <http://www.yourwindow.to/business-continuity/bcpindex.htm>**

## **COLLABORATION AND 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? Use Google Sites to post the results on the team's Web site.**

**There are literally dozens of products from different vendors that can be researched in answering this question. Below is some links to some of the more popular vendors and their product offerings.**

**<http://antivirus-software.6starreviews.com/?Refer=Goog&Keyword=antivirus%20software>**

**<http://www.symantecstore.com>**

**<http://mcafee.com>**

<http://www.pandasecurity.com>  
<http://www.trendmicro.com>

## LEARNING TRACK MODULE

1. *The Booming Job Market in IT Security*
2. *The C-SOX Act*
3. *Computer Forensics*
4. *General and Application Controls for Information Systems*
5. *Security Vulnerability and Reliability*
6. *Management Challenges of Security and Control*

Students will find Learning Track Modules on these topics at the MyMISLab for this chapter.

## HANDS-ON MIS: PROJECTS

### Management Decision Problems

**1. K2 Network:** operates online game sites that accommodate millions of players at once and played simultaneously by people all over the world. Prepare a security analysis for this Internet-based business. What kinds of threats should it anticipate? What would be their impact on the business? What steps can it take to prevent damage to its Web sites and continuing operations?

Threats include:

Hackers and crackers

File sharing over peer-to-peer networks

Malware including worms and Trojan horses

Denial-of-service attacks

Botnet attacks on network servers

The company should determine the impact on its business by performing a risk assessment. Business managers working with information systems specialists should determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage.

Steps the company can take to prevent damage include:

Access controls: prevent improper access to all of the organization's systems by unauthorized insiders and outsiders.

Firewalls: prevent unauthorized users from accessing private networks.

Intrusion detection systems: full-time monitoring tools placed at the most vulnerable

points or “hot spots” to detect and deter intruders.

Antivirus/antispyware: check computer systems and drives for the presence of computer viruses and spyware.

Unified threat management systems: combines all these tools into a single appliance.

Since this seems to be a relatively small company, a UTM system would make security management much easier.

Recovery-oriented computing: design the system to recover quickly and implement capabilities and tools to help operators pinpoint the sources of faults in multi-component system.

2. Security analysis statistics: analyze high risk, medium risk, and low risk vulnerabilities by type of computing platform.

#### SECURITY VULNERABILITIES BY TYPE OF COMPUTING PLATFORM

PLATFORM	NUMBER OF COMPUTERS	HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL VULNERABILITIES
Windows Server (corporate applications)	1	11	37	19	67
Windows Vista Ultimate (high-level administrators)	3	56	242	87	1155
Linux (e-mail and printing services)	1	3	154	98	255
Sun Solaris (UNIX) (E-commerce and Web servers)	2	12	299	78	778
Windows Vista Ultimate user desktops and laptops with office productivity tools that can also be linked to the corporate network running corporate applications and intranet	195	14	16	1,237	247,065

1. Calculate the total number of vulnerabilities for each platform. What is the potential impact of the security problems for each computing platform on the organization?



The total number of vulnerabilities for each platform is indicated in the far right column of the table.

Potential impact of the security problems for each computing platform

- **High risk vulnerabilities:** misuse of passwords allows hackers, crackers, and employees to access specific systems and files and steal data or change application programs; non-authorized users could change applications or enter corrupt or faulty data; unauthorized programs could corrupt data or programs
- **Medium risk vulnerabilities:** obviously it's not a good thing for users to be able to shut down systems – that should be restricted to high-level administrators; passwords and screen savers could allow viruses, worms, and Trojan horses to enter the system; outdated software versions make it more difficult to keep current software programs up-to-date and provide holes in which unauthorized users could enter a system
- **Low risk vulnerabilities:** user lack of knowledge is the single greatest cause of network security breaches. Password systems that are too easy or too difficult compromise system security and could create unintentional vulnerabilities from internal or external threats.

2. If you only have one information systems specialist in charge of security, which platforms should you address first in trying to eliminate these vulnerabilities? Second? Third? Last? Why?

First platform to protect: Windows Vista Ultimate (high-level administrators) – administrators usually have access to areas that no other users have. The tasks that administrators perform affect the core operations of a system.

Second Platform to protect: Windows Server (corporate applications) – if the corporate applications are down or corrupted, the entire organization will be unable to conduct business

Third platform to protect: Sun Solaris (UNIX) (E-commerce and Web servers) – after ensuring that internal operations are safe and secure, the next area to protect focuses on the ability to reach customers and for them to reach the company

- Fourth platform to protect: Windows Vista Ultimate user desktops and laptops – this area probably has fewer critical applications, files, and data than the corporate applications area.

Last platform to protect: Linux (e-mail and printing services) – while it may be critical to a few users, it's not likely the organization will suffer huge damage or losses if e-mail and print services are down for a while.

3. Identify the types of control problems illustrated by these vulnerabilities and explain the measures that should be taken to solve them.

- **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. General controls apply to all computerized applications

and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

- **Windows Vista Ultimate (high-level administrators)**
- **Sun Solaris (UNIX) (E-commerce and Web servers)**
- **Application controls:** 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 input controls, processing controls, and output controls.
  - **Windows Server (corporate applications)**
  - **Linux (e-mail and printing services)**
  - **Sun Solaris (UNIX) (E-commerce and Web servers)**
  - **Windows Vista Ultimate user desktops and laptops**
- Measures that should be taken to solve them include
  - Create a security policy and an acceptable use policy
  - Use authorization management systems
  - Create a business continuity plan
  - Complete an MIS audit that includes a security audit
  - Apply access controls, firewalls, antivirus/antispysware to system
  - Install an intrusion detection management system
  - Determine if fault-tolerant or high availability computing is necessary
  - 
  -

4. What does your firm risk by ignoring the security vulnerabilities identified?

**Information systems are vulnerable to technical, organizational, and environmental threats from internal and external sources. Managers at all levels must make system security and reliability their number one priority. They must also impress upon all employees how important security is throughout the system. There are several ways the business value of security and control can be measured:**

**the dollars a company spends to secure system**

**the amount of money spent to recover from system fraud and abuse**

**the lost revenue from system downtime**

**the amount of money spent on legal claims against a company if it experiences security breaches**

**the damage done to a company's reputation**

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

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

Remind students that setting security policies and procedures really means developing a plan for how to deal with computer security. One way to approach this task is:

- Look at what you are trying to protect
- Look at what you need to protect it from
- Determine how likely the threats are
- Implement measures that will protect your assets in a cost-effective manner
- Review the process continuously, and improve things every time a weakness is found

Students' reports should spend the most time on the last two steps, but the first three are critically important to making effective decisions about security. One old truism in security is that the cost of protecting yourself against a threat should be less than the cost recovering if the threat were to strike you. Without reasonable knowledge of what you are protecting and what the likely threats are, following this rule could be difficult.

Reports should note that the goal in developing an official site policy on computer security is to define the organization's expectations of proper computer and network use and to define procedures to prevent and respond to security incidents. In order to do this, aspects of the particular organization must be considered. First, the goals and direction of the organization should be considered. For example, a military base may have very different security concerns from those of a university. Second, the site security policy developed must conform to existing policies, rules, regulations and laws that the organization is subject to. Therefore, it will be necessary to identify these and take them into consideration while developing the policy. Third, unless the local network is completely isolated and standalone, it is necessary to consider security implications in a more global context. The policy should address the issues when local security problems develop as a result of a remote site as well as when problems occur on remote systems as a result of a local host or user.

Policy creation must be a joint effort by technical personnel, who understand the full ramifications of the proposed policy and the implementation of the policy, and by decision makers who have the power to enforce the policy. A policy that is neither implementable nor enforceable is useless. Since a computer security policy can affect everyone in an organization, it is worth taking some care to make sure the organization has the right level of authority involved in the policy decisions. Though a particular group (such as a campus information services group) may have responsibility for enforcing a policy, an even higher group may have to support and approve the policy. Establishing a site policy has the potential for involving every computer user at the site in a variety of ways. Computer users may be responsible for personal password administration. Systems managers are obligated to fix security holes and to oversee the system. It is critical to get the right set of people involved at the start of the process. There may already be groups concerned with security that would consider a computer security policy to be their area. Some of the types of groups that might be involved

include auditing/control, organizations that deal with physical security, campus information systems groups, and so forth. Asking these types of groups to “buy in” from the start can help facilitate the acceptance of the policy.

Mercer Paints Risk Assessment		
Exposure	Probability of Occurrence (%)	Average Losses
Virus 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 Usage by Employees	5	\$5,000
Power Failure	15	\$300,000

The solution for this exercise is found in the file named Ch08\_Security\_Risk\_Assessment.xls in the Chapter 8 folder.

## IMPROVING DECISION MAKING: EVALUATING SECURITY OUTSOURCING SERVICES

**Software skills:** Web browser and presentation software

**Business skills:** Evaluating business outsourcing services

Data and network security are major challenges, and many companies have taken actions to protect their equipment and access to their data. Some of those companies have chosen to outsource that function rather than train their own staff or hire specialists from outside their company. Finding security outsourcing services can be difficult, although finding sources that help you decide whether or not to outsource is much easier. In both cases, use several search engines to find sources that can help you decide whether to outsource and to locate companies that offer outsourcing of computer security.

**As an information systems expert in your firm, you have been assigned the following tasks.**

- 1. Present a brief summary of the arguments for and against outsourcing system security for your company.**
- 2. Select two firms that offer system security outsourcing services, and compare them and their services.**
- 3. Prepare an electronic presentation for management summarizing your findings. Your presentation should make the case on whether or not your company should outsource system security. If you believe your**

**company should outsource, the presentation should identify which security outsourcing service should be selected and justify your selection.**

**Your students will provide several pros and cons to outsourcing. Most of them will conclude that the major pro would be a financial savings. As a con, they may say that finding a reliable contractor is not always an easy thing to do. Four companies that are proven business leaders are: Ansotech, Inc., Foundstone Enterprise, Counterpane Internet Security, and Panurgy.**

## **CASE STUDY: A ROGUE TRADER AT SOCIÉTÉ GÉNÉRALE ROILS THE WORLD FINANCIAL SYSTEM**

### **1. What concepts in this chapter are illustrated in this case?**

Chapter concepts illustrated in this case include:

- System vulnerabilities:
  - Computer crime: using computers as instruments of crime to defraud the bank, customers, and other financial institutions
  - Internal threats from employees: Kerviel has access to privileged information; he was able to run through the organization's system without leaving a trace
- Business value of security and control:
  - Organizations 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
  - Had Kerviel committed his actions in the U.S. he would have violated the Sarbanes-Oxley Act. Organizational executives could have been held criminally liable.
- Information system 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
  - Application controls: automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application
- Risk assessment: determines the level of risk to the firm if a specific activity or process is not properly controlled
- 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

- The role of auditing: an MIS audit examines the firm's overall security environment as well as controls governing individual information systems

**2. Describe the control weaknesses at SocGen. What management, organization, and technology factors contributed to those weaknesses?**

One former SocGen risk auditor, Maxime Legrand, called the control procedures used to monitor the activity of its traders a sham and that the management “pretend(s) to have an inspection to please the banking commission.”

**Management:** Kerviel's supervisors saw a balanced book when in fact he was exposing the bank to substantial risk because of the way he entered the transactions. Kerviel worked late into the night long after other traders had gone home and took only four vacation days over the course of 2007 to prevent his activities from being detected. Managers did not enforce vacation policies that would have allowed them to scrutinize his work while he was gone. Supposedly he used his manager's computer to execute several of his fraudulent trades while the manager watched him. Kerviel's defense lawyers argue that he acted with the tacit approval of his superiors during his more successful initial period of fraudulent activity.

**Organization:** Kerviel gained familiarity with many of the company's security procedures and back-office systems. He was then moved to another job in the company in which he could use that knowledge. He knew the schedule of SocGen's internal controls which allowed him to eliminate his fake trades from the system just minutes prior to the scheduled checks and re-enter them soon after. The temporary imbalance did not trigger an alert. The bank ignored many warning signs that Kerviel was capable of the level of fraud that he committed. The bank failed to follow up on 75 warnings on Kerviel's positions over the course of several years.

**Technology:** Kerviel was able to use other employees' access codes and user information to enter fake trades. The system failed to detect that Kerviel performed legitimate transaction in one direction, but falsified the hedges that were supposed to 'offset' the legitimate ones. He entered false transactions in a separate portfolio, distinct from the one containing his real trades. No system detection software was installed to detect these transactions. SocGen's controls were capable of detecting more complicated errors and fraudulent transaction than the simple ones that Kerviel allegedly committed.

**3. Who should be held responsible for Kerviel's trading losses? What role did SocGen's systems play? What role did management play?**

Most students will probably argue that managers and executives at SocGen should be held responsible for Kerviel's trading losses. They are the ones who should be setting policies and enforcing them to prevent these kinds of activities from taking place.

SocGen's systems were capable of detecting complicated errors and fraudulent transactions that were more sophisticated than those committed by Kerviel. Yet he was able to commit very simple fraudulent transactions that went undetected. System controls obviously were not as thorough or as strong as they should have been. There were several other system vulnerabilities that Kerviel was able to exploit to commit his crime.

Managers aided Kerviel's activities by deciding to unload his positions soon after discovering the fraud, despite the fact that the market conditions at the time were decidedly unfavourable. That led to even greater problems in the global financial world. The SEC launched an investigation into whether or not SocGen violated U.S. securities laws by unwinding Kerviel's positions covertly after the fraud was revealed as well as whether or not insider information played a role in the selling of SocGen stock prior to the announcement of the scandal.

#### **4. What are some ways SocGen could have prevented Kerviel's fraud?**

Some of the ways SocGen could have prevented Kerviel's fraud include:

- Instituting access controls to prevent improper access to systems by unauthorized insiders and outsiders. The bank could have used authentication technologies like tokens, smart cards, or biometric authorization instead of simple passwords. That would have prevented Kerviel from being able to use other employees' access codes to enter transactions.
- Intrusion detection systems could have been installed that would have detected much of Kerviel's activities. These systems generate alarms if they find a suspicious or anomalous event. They also check to see if important files have been modified. Monitoring software examines events as they are happening to discover security attacks in progress. Many of Kerviel's false 'offsetting' transactions could have been detected using one of these systems.
- Stronger auditing procedures should have been in place and enforced. Auditors can trace the flow of sample transactions through the system and perform tests, using automated audit software.
- Using computer forensic techniques and technologies would have helped. Electronic evidence resides on computer storage media in the form of computer files and as ambient data which are not visible to the average user. Data that Kerviel deleted on the bank's storage media could have been recovered through various techniques. The data could have been used as evidence at his trial and in follow-up investigations.

#### **5. If you were responsible for redesigning SocGen's systems, what would you do to address their control problems?**

Student answers will vary but should address these elements:

**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. These controls address software controls, physical hardware controls, computer operations controls, data security controls, controls over implements of system processes, and administrative controls. Table 8-3 describes each of these controls. SocGen is in need of most of these.

**Application controls:** specific controls unique to each computerized application. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by applications. Application controls include input controls, processing controls, and output controls.

**Acceptable use policy:** SocGen should create an AUP to define acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

**Authorization management system:** establishes 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.