organization understand and appreciate information security risks that they will authorize their IT department to develop an effective set of controls.

Most directors in the U.S. government do not have people in their organizations with the expertise and power to make changes, and many staff members are just not right for the job. OPM director Katherine Archuleta had formerly been the National Political Director for Barak Obama's 2012 presidential reelection campaign. CIO Donna Seymour, who was supposed to advise Archuleta on how to manage risk in IT systems, was a career government employee for more than 34 years. She had some IT and management roles at the Department of Defense and other agencies and has a degree in computer science but no specific expertise in cybersecurity. It is also difficult to bring in experienced managers from the business world because federal government pay scales are so low. A chief information officer (CIO) or chief information security officer (CISO) in the federal government would probably be paid about $168,000 annually, whereas an equivalent position in the private sector would probably have annual compensation of $400,000.

Since the OPM break-in, there has been a massive effort to rectify years of poor IT management. OPM is moving toward more centralized management of security. Information system security officers (ISSOs) report directly to a CISO. These positions are filled by individuals with professional security backgrounds. OPM hired a cybersecurity advisor, Clifton Triplett, and increased its IT modernization budget from $31 million to $87 million, with another $21 million scheduled for 2016.

OPM told current and former federal employees they could have free credit monitoring for 18 months to make sure their identities had not been stolen, but it has been slapped with numerous lawsuits from victims. Seymour faces a lawsuit for her role in failing to protect millions of personal employee data files, and Archuleta had to resign.

The FBI and Department of Homeland Security released a "cyber alert" memo describing lessons learned from the OPM hack. The memo lists generally recommended security practices for OPM to adopt, including encrypting data, activating a personal firewall at agency workstations, monitoring users' online habits, and blocking potentially malicious sites. The Obama administration ordered a 30-day Cybersecurity Sprint across all agencies to try to fix the big problems. Without a strong foundation, this investment could prove futile in the long run. OPM and the federal government as a whole need to invest more in managers with IT security expertise and give those individuals real authority to act.

The Obama administration is trying to determine whether other federal agencies storing sensitive information have weak protection. An audit issued before the Chinese attacks pointed to lax security at the Internal Revenue Service, the Nuclear Regulatory Commission, the Energy Department, the Securities and Exchange Commission, and even the Department of Homeland Security, which is responsible for securing the nation's critical networks and infrastructure. Computer security failure remains across agencies even though the government has spent at least $65 billion on security since 2006.

Sources: Sean Lyngaas, "What DHS and the FBI Learned from the OPM Breach," *FCW*, January 11, 2016; Adam Rice, "Warnings, Neglect and a Massive OPM Breach," SearchSecurity.com, accessed June 15, 2016; Steve Rosenbush, "The Morning Download: Outdated Tech Infrastructure Led to Massive OPM Breach," *Wall Street Journal*, July 10, 2015; Mark Mazzette and David E. Sanger, "U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies," *New York Times,* July 24, 2015; Damian Paletta and Danny Yadron, "OPM Ratches Up Estimate of Hack's Scope" *Wall Street Journal*, July 9, 2015; David E. Sanger, Nicole Perlroth, and Michael D. Shear, "Attack Gave Chinese Hackers Privileged Access to U.S. Systems," *New York Times*, June 20, 2015; and David E. Sanger and Julie Hirschfield, "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, June 4, 2015.

CASE STUDY QUESTIONS

8-13 List and describe the security and control weaknesses at OPM that are discussed in this case.

8-14 What management, organization, and technology factors contributed to these problems? How much was management responsible?

8-15 What was the impact of the OPM hack?

8-16 Is there a solution to this problem? Explain your answer.

MyMISLab

Go to the Assignments section of MyMISLab to complete these writing exercises.

8-17 Describe three spoofing tactics employed in identity theft by using information systems.

8-18 Describe four reasons mobile devices used in business are difficult to secure.

The hackers' biggest prize was probably more than 20 years of background check data on the highly sensitive 127-page Standard Forms SF-86 Questionnaire for National Security Positions. SF-86 forms contain information about family members, college roommates, foreign contacts, and psychological information. OPM systems containing information related to the background investigations of current, former, and prospective federal government employees, including U.S. military personnel, and those for whom a federal background investigation was conducted, may have been extracted. Government officials say that the exposure of security clearance information could pose a problem for years.

The Central Intelligence Agency (CIA) does not use the OPM system, and its records were protected during the breach. However, intelligence and congressional officials worried that the hackers or Chinese intelligence operatives could still use the detailed OPM information they did obtain to identify U.S. spies by process of elimination. If they combined the stolen data with other information gathered over time, they could use big data analytics to identify operatives.

The potential exposure of U.S. intelligence officers could prevent many of them from ever being posted abroad again. Adm. Michael S. Rogers, director of the National Security Agency, suggested that the personnel data could also be used to develop "spear phishing" attacks on government officials. In such attacks, victims are duped into clicking on what appear to be e-mails from people they know, allowing malware into their computer networks.

The stolen data also included 5.6 million sets of fingerprints. According to biometrics expert Ramesh Kesanupalli, this could compromise secret agents because they could be identified by their fingerprints even if their names had been changed.

The OPM had been warned multiple times of security vulnerabilities and failings. A March 2015 OPM Office of the Inspector General semiannual report to Congress mentioned persistent deficiencies in OPM's information system security program, including incomplete security authorization packages, weaknesses in testing information security controls, and inaccurate plans of action and milestones.

Security experts have stated that the biggest problem with the breach was not OPM's failure to prevent remote break-ins but the absence of mechanisms to detect outside intrusion and inadequate encryption of sensitive data. Assistant Secretary for Cybersecurity and Communications Andy Ozment pointed out that if someone has the credentials of a user on the network, then he or she can access data even if they are encrypted, so encryption in this instance would not have protected the OPM data.

OPM was saddled with outdated technology and weak management. A DHS Federal Information Security Management Act (FISMA) Audit for fiscal year 2014 and audit of the Office of the Inspector General found serious flaws in OPM's network and the way it was managed. OPM did not maintain an inventory of systems and baseline configurations, with 11 servers operating without valid authorization. The auditors could not independently verify OPM's monthly automated vulnerability scanning program for all servers. There was no senior information security specialist or chief information security officer (CISO) responsible for network security. OPM lacked an effective multifactor authentication strategy and had poor management of user rights, inadequate monitoring of multiple systems, many unpatched computers, and a decentralized and ineffective cybersecurity function. Sensitive data were unencrypted and stored in old database systems that were vulnerable. What's more, OPM used contractors in China to manage some of its databases. These deficiencies had been pointed out to OPM over and over again since a FISMA audit in 2007. OPM had the vulnerabilities, no security-oriented leadership, and a skillful and motivated adversary.

Some security experts see OPM's vulnerabilities as a sign of the times, a reflection of large volumes of data, contemporary network complexity, weak organizational and cultural practices, and a legacy of outdated and poorly written software. As Thomas Bayer, CIO at Standard & Poor's Ratings, explained, until you have a serious data breach like the OPM hack, everyone invests in other things. It's only when a massive data breach occurs that organizations focus on their infrastructure. The expertise and technology for halting or slowing down cyberattacks such as that on OPM are not a mystery, and many companies and some government organizations are effectively defending themselves against most of the risks they face.

OPM lacked leadership and accountability. The prevailing mentality was for everyone to sit and bide their time. The CEO, CIO, and CISO in a private organization would be held accountable by the board of directors.

OPM is a top-heavy organization, with a large management layer of senior advisers to the director. For example, CIO Donna Seymour has 28 staff members under her and four direct reporting organizations, none of which is security-focused. There is no listed CISO function. OPM's director has 62 senior leaders in four groups. Many OPM managers are politically appointed and lack the expertise to make informed decisions about cybersecurity. It's only when managers in an

Improving Decision Making: Evaluating Security Outsourcing Services

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

8-11 This project will help develop your Internet skills in using the web to research and evaluate security outsourcing services.

You have been asked to help your company's management decide whether to outsource security or keep the security function within the firm. Search the web to find information to help you decide whether to outsource security and to locate security outsourcing services.

- Present a brief summary of the arguments for and against outsourcing computer security for your company.
- Select two firms that offer computer security outsourcing services and compare them and their services.
- Prepare an electronic presentation for management, summarizing your findings. Your presentation should make the case of whether your company should outsource computer security. If you believe your company should outsource, the presentation should identify which security outsourcing service you selected and justify your decision.

Collaboration and Teamwork Project

Evaluating Security Software Tools

8-12 With a group of three or four students, use the web to research and evaluate security products from two competing vendors, such as for antivirus software, firewalls, or antispyware software. For each product, describe its capabilities, for what types of businesses it is best suited, and its cost to purchase and install. Which is the best product? Why? If possible, use Google Docs and Google Drive or Google Sites to brainstorm, organize, and develop a presentation of your findings for the class.

U.S. Office of Personnel Management Data Breach: No Routine Hack

CASE STUDY

The U.S. Office of Personnel Management (OPM) is responsible for recruiting and retaining a world-class workforce to serve the American people and is also responsible for background investigations on prospective employees and security clearances. In June 2015, the OPM announced that it had been the target of a data breach targeting the records of as many as 4 million people. In the following months, the number of stolen records was upped to 21.5 million. This was no routine hack. Federal officials believe this data breach is among the largest breaches of government data in U.S. history

Information targeted in the breach included personally identifiable information such as social security numbers as well as names, dates and places of birth, and addresses. Also stolen was detailed security clearance–related background information. This included records of people who had undergone background checks but who were not necessarily current or former government employees.

The data breach is believed to have begun in March 2014 and perhaps earlier, but it was not noticed by the OPM until April 2015, and it is unclear how it was actually discovered. The intrusion occurred before OPM had finished implementing new security procedures that restricted remote access for network administrators and reviewed all Internet connections to the outside world.

U.S. government officials suspect that the breach was the work of Chinese hackers, although there is no proof that it was actually sponsored by the Chinese government. Chinese officials have denied involvement. The attackers had stolen user credentials from contractor KeyPoint Government Solutions to access OPM networks, most likely through social engineering. The hackers then planted malware, which installed itself within OPM's network and established a backdoor for plundering data. From there, attackers escalated their privileges to gain access to a wide range of OPM systems.

Discussion Questions

8-5 MyMISLab Security isn't simply a technology issue, it's a business issue. Discuss.

8-6 MyMISLab If you were developing a business continuity plan for your company, where would you start? What aspects of the business would the plan address?

8-7 MyMISLab Suppose your business had an e-commerce website where it sold goods and accepted credit card payments. Discuss the major security threats to this website and their potential impact. What can be done to minimize these threats?

Hands-On MIS Projects

The projects in this section give you hands-on experience analyzing security vulnerabilities, using spreadsheet software for risk analysis, and using web tools to research security outsourcing services. Visit MyMISLab's Multimedia Library to access this chapter's Hands-On MIS Projects.

Management Decision Problems

8-8 Reloaded Games is an online games platform that powers leading massively multiplayer online games. The Reloaded platform serves more than 30 million users. The games can accommodate millions of players at once and are 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 websites and continuing operations?

8-9 A survey of your firm's IT infastructure has identified a number of security vulnerabilities. Review the data about these vulnerabilities, which can be found in a table in MyMISLab. Use the table to answer the following questions:

- 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?
- 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?
- Identify the types of control problems these vulnerabilities illustrate and explain the measures that should be taken to solve them.
- What does your firm risk by ignoring the security vulnerabilities identified?

Improving Decision Making: Using Spreadsheet Software to Perform a Security Risk Assessment

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

8-10 This project uses spreadsheet software to calculate anticipated annual losses from various security threats identified for a small company.

Mercer Paints is a paint manufacturing company located in Alabama that uses a network to link its business operations. A security risk assessment that management requested identified a number of potential exposures. These exposures, their associated probabilities, and average losses are summarized in a table, which can be found in MyMISLab. Use the table to answer the following questions:

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

Ransomware, 300
Risk assessment, 310
Sarbanes-Oxley Act, 308
Secure Hypertext Transfer Protocol (S-HTTP), 320
Secure Sockets Layer (SSL), 320
Security, 295
Security policy, 313
Smart card, 317
Sniffer, 301
Social engineering, 305
Spoofing, 301
Spyware, 300
SQL injection attack, 300
Token, 316
Trojan horse, 300
Two-factor authentication, 317
Unified threat management (UTM), 320
War driving, 297
Worms, 298
Zero-day vulnerabilities, 306

MyMISLab

To complete the problems with the MyMISLab, go to EOC Discussion Questions in the MyMISLab.

Review Questions

8-1 Why are information systems vulnerable to destruction, error, and abuse?

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

8-2 What is the business value of security and control?

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

8-3 What are the components of an organizational framework for security and control?

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

8-4 What are the most important tools and technologies for safeguarding information resources?

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

8-2 *What is the business value of security and control?*

Lack of sound security and control can cause firms relying on computer systems for their core business functions to lose sales and productivity. Information assets, such as confidential employee records, trade secrets, or business plans, lose much of their value if they are revealed to outsiders or if they expose the firm to legal liability. 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.

8-3 *What are the components of an organizational framework for security and control?*

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

8-4 *What are the most important tools and technologies for safeguarding information resources?*

Firewalls prevent unauthorized users from accessing a private network when it is linked to the Internet. Intrusion detection systems monitor private networks for 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; antispyware software combats intrusive and harmful spyware programs. Encryption, the coding and scrambling of messages, is a widely used technology for securing electronic transmissions over unprotected networks. Digital certificates combined with public key encryption provide further protection of electronic transactions by authenticating a user's identity. Companies can use fault-tolerant computer systems to make sure that their information systems are always available. Use of software metrics and rigorous software testing help improve software quality and reliability.

Key Terms

Acceptable use policy (AUP), 313
Antivirus software, 319
Application controls, 309
Authentication, 316
Biometric authentication, 317
Botnet, 301
Bugs, 306
Business continuity planning, 315
Click fraud, 304
Computer crime, 302
Computer forensics, 308
Computer virus, 298
Controls, 295
Cybervandalism, 301
Cyberwarfare, 305
Deep packet inspection (DPI), 322
Denial-of-service (DoS) attack, 301
Digital certificates, 321
Disaster recovery planning, 314
Distributed denial-of-service (DDoS) attack, 301
Downtime, 322
Drive-by download, 299
Encryption, 320
Evil twin, 303
Fault-tolerant computer systems, 322
Firewall, 318
General controls, 309
Gramm-Leach-Bliley Act, 308
Hacker, 301
HIPAA, 307
Identity management, 313
Identity theft, 303
Information systems audit, 315
Intrusion detection systems, 319
Keyloggers, 300
Malware, 298
Managed security service providers (MSSPs), 323
Online transaction processing, 322
Password, 316
Patches, 306
Pharming, 303
Phishing, 303
Public key encryption, 320
Public key infrastructure (PKI), 322

Google Play now provides security scanning of all applications before they are available to download, ongoing security checks for as long as the application is available, and a Verify Apps service for mobile device protection for apps installed outside of Google Play. However, these Android improvements are largely only for people who use a phone or tablet running a newer version of Android and restrict their app downloads to Google's own Play store.

Companies need to develop mobile security strategies that strike the right balance between improving worker productivity and effective information security. Aetna's Chief Security Officer (CSO) Jim Routh says there is a certain minimum level of mobile security he requires regardless of whether a device is company- or personally owned. Aetna has about 6,000 users equipped with mobile devices that are either personally owned or issued by the company. Each device has mandatory protection that provides an encrypted channel to use in unsecured Wi-Fi networks and alerts the user and the company if a malicious app is about to be installed on the device.

Colin Minihan, director of security and best practices at VMWare AirWatch, believes that understanding users and their needs helps a mobile security strategy progress further. VmAirWatch categorizes similar groups of users and devises a specific plan of action for each group, choosing the right tools for the job.

According to Patrick Hevesi, Nordstrom's former director of security, if users need access to critical corporate data that must be protected, the firm should probably allow only fully managed, fully controlled, approved types of devices. Users who only want mobile tools for e-mail and contacts can more easily bring their own devices. The key questions to ask are called the "three Ws": Who needs access? What do they need to access? What is the security posture of the device?

Sources: Michael Heller, "Mobile Security Strategy Matures with BYOD," and Kathleen Richards, "CISOs Battle to Control Mobile Risk in the Workplace," *Information Security Magazine,* June 1, 2016; Nathan Olivarez-Giles, "Android's Security Improves—for the Few," *Wall Street Journal,* April 21, 2016; Ponemon Institute, "The Economic Risk of Confidential Data on Mobile Devices in the Workplace," February, 2016; McAfee Inc., "Mobile Threat Report: What's on the Horizon for 2016," 2016; Charlie Osborne, "Dropbox Patches Android Security Flaw," *Zero Day,* March 11, 2015; Edel Creely, "5 BYOD Security Implications and How to Overcome Them," Trilogy Technologies, May 26, 2015; Tony Kontzer, "Most of Your Mobile Apps Have Been Hacked," *Baseline,* January 16, 2015; and Ponemon Institute, Global Study on Mobility Risks (February 2012).

CASE STUDY QUESTIONS

1. It has been said that a smartphone is a computer in your hand. Discuss the security implications of this statement.
2. What kinds of security problems do mobile computing devices pose?
3. What management, organizational, and technology issues must be addressed by smartphone security?
4. What steps can individuals and businesses take to make their smartphones more secure?

Review Summary

8-1 *Why are information systems vulnerable to destruction, error, and abuse?*

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

INTERACTIVE SESSION: TECHNOLOGY

BYOD: A Security Nightmare?

Bring your own device has become a huge trend, with half of employees with mobile computing tools at workplaces worldwide using their own devices. This figure is expected to increase even more in the years to come. But while use of the iPhone, iPad, and other mobile computing devices in the workplace is growing, so are security problems. Quite a few security experts believe that smartphones and other mobile devices now pose one of the most serious security threats for organizations today.

Whether mobile devices are company-assigned or employee-owned, they are opening up new avenues for accessing corporate data that need to be closely monitored and protected. Sensitive data on mobile devices travel, both physically and electronically, from the office to home and possibly other off-site locations. According to a February 2016 Ponemon Institute study of 588 U.S. IT and security professionals, 67 percent of those surveyed reported that it was certain or likely that an employee's mobile access to confidential corporate data had resulted in a data breach. Unfortunately, only 41 percent of respondents said their companies had policies for accessing corporate data from mobile devices.

More than half of security breaches occur when devices are lost or stolen. That puts all of the personal and corporate data stored on the device, as well as access to corporate data on remote servers, at risk. Physical access to mobile devices may be a greater threat than hacking into a network because less effort is required to gain entry. Experienced attackers can easily circumvent passwords or locks on mobile devices or access encrypted data. Moreover, many smartphone users leave their phones totally unprotected to begin with or fail to keep the security features of their devices up-to-date. In the Websense and the Ponemon Institute's Global Study on Mobility Risks, 59 percent of respondents reported that employees circumvented or disabled security features such as passwords and key locks.

Another worry today is large-scale data leakage caused by use of cloud computing services. Employees are increasingly using public cloud services such as Google Drive or Dropbox for file sharing and collaboration. Valiant Entertainment, Cenoric Projects, Vita Coco, and BCBGMAXAZRIAGROUP are among the companies allowing employees and freelance contractors to use Dropbox for Business to post and share files. There are also many instances where employees are using Dropbox to store and exchange files without their employers' approval. In early 2015 Dropbox had to patch a security flaw that allowed cyberattackers to steal new information uploaded to accounts through compromised third-party apps that work with Dropbox services on Android devices. There's very little a company can do to prevent employees who are allowed to use their smartphones from downloading corporate data so they can work on those data remotely.

Text messaging and other mobile messaging technologies are being used to deliver all kinds of scam campaigns, such as adult content and rogue pharmacy, phishing, and banking scams, and text messages have been a propagation medium for Trojan horses and worms. A malicious source is now able to send a text message that will open in a mobile browser by default, which can be readily utilized to exploit the recipient.

To date, deliberate hacker attacks on mobile devices have been limited in scope and impact, but this situation is worsening. Android is now the world's most popular operating system for mobile devices with 81 percent of the global market, and most mobile malware is targeted at the Android platform. When corporate and personal data are stored on the same device, mobile malware unknowingly installed by the user could find its way onto the corporate network.

Apple uses a closed "walled garden" model for managing its apps and reviews each one before releasing it on its App Store. Android application security has been weaker than that for Apple devices, but it is improving. Android application security uses sandboxing, which confines apps, minimizing their ability to affect one another or manipulate device features without user permission. Google removes any apps that break its rules against malicious activity from Google Play, its digital distribution platform that serves as the official app store for the Android operating system. Google also vets the backgrounds of developers. Recent Android security enhancements include assigning varying levels of trust to each app, dictating what kind of data an app can access inside its confined domain, and providing a more robust way to store cryptographic credentials used to access sensitive information and resources.

Securing Mobile Platforms

If mobile devices are performing many of the functions of computers, they need to be secured like desktops and laptops against malware, theft, accidental loss, unauthorized access, and hacking attempts. The Interactive Session on Technology describes these mobile vulnerabilities in greater detail and their implications for both individuals and businesses.

Mobile devices accessing corporate systems and data require special protection. Companies should make sure that their corporate security policy includes mobile devices, with additional details on how mobile devices should be supported, protected, and used. They will need mobile device management tools to authorize all devices in use; to maintain accurate inventory records on all mobile devices, users, and applications; to control updates to applications; and to lock down or erase lost or stolen devices so they can't be compromised. Data loss prevention technology can identify where critical data are saved, who is accessing the data, how data are leaving the company, and where the data are going. Firms should develop guidelines stipulating approved mobile platforms and software applications as well as the required software and procedures for remote access of corporate systems. The organization's mobile security policy should forbid employees from using unsecured, consumer-based applications for transferring and storing corporate documents and files or sending such documents and files to oneself by e-mail without encryption.

Companies should encrypt communication whenever possible. All mobile device users should be required to use the password feature found in every smartphone. Mobile security products are available from Kaspersky, Symantec, Trend Micro, and McAfee.

Ensuring Software Quality

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

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

Good testing begins before a software program is even written, by using a *walkthrough*—a review of a specification or design document by a small group of people carefully selected based on the skills needed for the particular objectives being tested. When developers start writing software programs, coding walkthroughs can also be used to review program code. However, code must be tested by computer runs. When errors are discovered, the source is found and eliminated through a process called *debugging*. You can find out more about the various stages of testing required to put an information system into operation in Chapter 13. Our Learning Tracks also contain descriptions of methodologies for developing software programs that contribute to software quality.

Security Outsourcing

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

Security Issues for Cloud Computing and the Mobile Digital Platform

Although cloud computing and the emerging mobile digital platform have the potential to deliver powerful benefits, they pose new challenges to system security and reliability. We now describe some of these challenges and how they should be addressed.

Security in the Cloud

When processing takes place in the cloud, accountability and responsibility for protection of sensitive data still reside with the company owning that data. Understanding how the cloud computing provider organizes its services and manages the data is critical.

Cloud computing is highly distributed. Cloud applications reside in large remote data centers and server farms that supply business services and data management for multiple corporate clients. To save money and keep costs low, cloud computing providers often distribute work to data centers around the globe where work can be accomplished most efficiently. When you use the cloud, you may not know precisely where your data are being hosted.

The dispersed nature of cloud computing makes it difficult to track unauthorized activity. Virtually all cloud providers use encryption, such as SSL, to secure the data they handle while the data are being transmitted. However, if the data are stored on devices that also store other companies' data, it's important to ensure that these stored data are encrypted as well. According to research from Alert Logic, there has been a 45 percent year-over-year increase in attacks on the cloud. DDoS attacks are especially harmful because they render cloud services unavailable to legitimate customers.

Companies expect their systems to be running 24/7. Cloud providers still experience occasional outages, but their reliability has increased to the point where a number of large companies are using cloud services for part of their IT infrastructures. Most keep their critical systems in-house.

Cloud users need to confirm that regardless of where their data are stored, they are protected at a level that meets their corporate requirements. They should stipulate that the cloud provider store and process data in specific jurisdictions according to the privacy rules of those jurisdictions. Cloud clients should find how the cloud provider segregates their corporate data from those of other companies and ask for proof that encryption mechanisms are sound. It's also important to know how the cloud provider will respond if a disaster strikes, whether the provider will be able to restore your data completely, and how long this should take. Cloud users should also ask whether cloud providers will submit to external audits and security certifications. These kinds of controls can be written into the service level agreement (SLA) before signing with a cloud provider. The Cloud Security Alliance (CSA) has created industrywide standards for cloud security, specifying best practices to secure cloud computing.

certificate system uses a trusted third party, known as a certificate authority (CA), to validate a user's identity. There are many CAs in the United States and around the world, including Symantec, GoDaddy, and Comodo.

The CA verifies a digital certificate user's identity offline. This information is put into a CA server, which generates an encrypted digital certificate containing owner identification information and a copy of the owner's public key. The certificate authenticates that the public key belongs to the designated owner. The CA makes its own public key available either in print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it was issued by the CA, and then obtains the sender's public key and identification information contained in the certificate. By using this information, the recipient can send an encrypted reply. The digital certificate system would enable, for example, a credit card user and a merchant to validate that their digital certificates were issued by an authorized and trusted third party before they exchange data. **Public key infrastructure (PKI)**, the use of public key cryptography working with a CA, is now widely used in e-commerce.

Ensuring System Availability

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

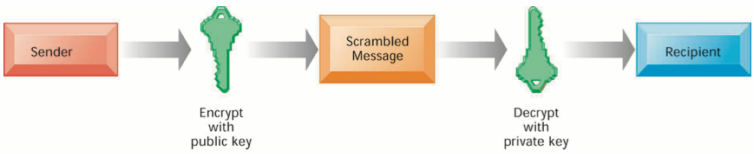
Fault-tolerant computer systems contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. Parts from these computers can be removed and repaired without disruption to the computer or downtime. **Downtime** refers to periods of time in which a system is not operational.

Controlling Network Traffic: Deep Packet Inspection

Have you ever tried to use your campus network and found that it was very slow? It may be because your fellow students are using the network to download music or watch YouTube. Bandwith-consuming applications such as file-sharing programs, Internet phone service, and online video can clog and slow down corporate networks, degrading performance. For example, Ball State University in Muncie, Indiana, found its network had slowed because a small minority of students were using P2P file-sharing programs to download movies and music.

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

FIGURE 8.6 PUBLIC KEY ENCRYPTION

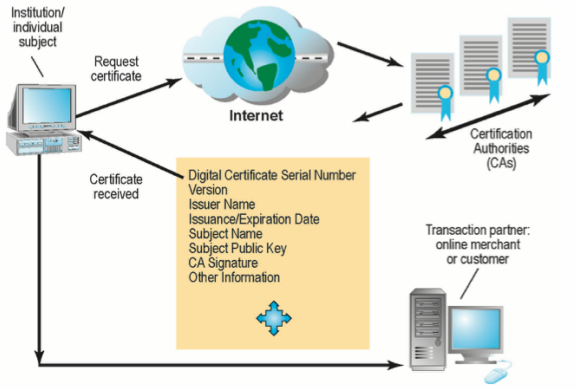


A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form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

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called **public key encryption** uses two keys: one shared (or public) and one totally private as shown in Figure 8.6. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory, and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions (see Figure 8.7). A digital

FIGURE 8.7 DIGITAL CERTIFICATES



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

Unified Threat Management Systems

To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and web content filtering and anti-spam software. These comprehensive security management products are called **unified threat management (UTM)** systems. UTM products are available for all sizes of networks. Leading UTM vendors include Fortinent, Sophos, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their products.

Securing Wireless Networks

The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy (WEP), is not very effective because its encryption keys are relatively easy to crack. WEP provides some margin of security, however, if users remember to enable it. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

In June 2004, the Wi-Fi Alliance industry trade group finalized the 802.11i specification (also referred to as Wi-Fi Protected Access 2 or WPA2) that replaces WEP with stronger security standards. Instead of the static encryption keys used in WEP, the new standard uses much longer keys that continually change, making them harder to crack.

Encryption and Public Key Infrastructure

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

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

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

Two methods of encryption are symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length. Today, a typical key will be 56 to 256 bits long (a string of from 56 to 256 binary digits) depending on the level of security desired. The longer the key, the more difficult it is to break the key. The downside is that the longer the key, the more computing power it takes for legitimate users to process the information.

Address Translation, and application proxy filtering. They are frequently used in combination to provide firewall protection.

Packet filtering examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation. This filtering technology can miss many types of attacks.

Stateful inspection provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver. It sets up state tables to track information over multiple packets. Packets are accepted or rejected based on whether they are part of an approved conversation or attempting to establish a legitimate connection.

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

Application proxy filtering examines the application content of packets. A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall. If a user outside the company wants to communicate with a user inside the organization, the outside user first communicates with the proxy application, and the proxy application communicates with the firm's internal computer. Likewise, a computer user inside the organization goes through the proxy to talk with computers on the outside.

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

Intrusion Detection Systems

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

Antivirus and Antispyware Software

Defensive technology plans for both individuals and businesses must include anti-malware protection for every computer. **Antivirus software** prevents, detects, and removes malware, including computer viruses, computer worms, Trojan horses, spyware, and adware. However, most antivirus software is effective only against malware already known when the software was written. To remain effective, the antivirus software must be continually updated. Even then it is not always effective because some malware can evade antivirus detection. Organizations need to use additional malware detection tools for better protection.

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.

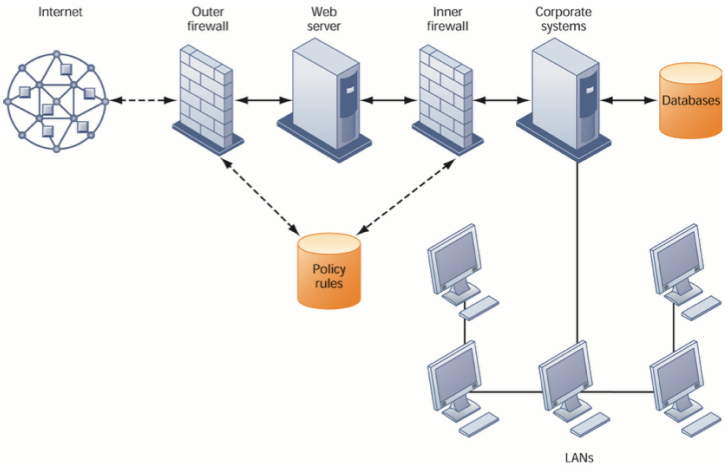
Firewalls

Firewalls prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network (see Figure 8.5).

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

In large organizations, the firewall often resides on a specially designated computer separate from the rest of the network, so no incoming request directly accesses private network resources. There are a number of firewall screening technologies, including static packet filtering, stateful inspection, Network

FIGURE 8.5 A CORPORATE FIREWALL



The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

display passcodes that change frequently. A **smart card** is a device about the size of a credit card that contains a chip formatted with access permission and other data. (Smart cards are also used in electronic payment systems.) A reader device interprets the data on the smart card and allows or denies access.

Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices to grant or deny access. Biometric authentication is based on the measurement of a physical or behavioral trait that makes each individual unique. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored profile of these characteristics to determine any differences between these characteristics and the stored profile. If the two profiles match, access is granted. Fingerprint and facial recognition technologies are just beginning to be used for security applications, with many PC laptops (and some smartphones) equipped with fingerprint identification devices and several models with built-in webcams and face recognition software.

The steady stream of incidents in which hackers have been able to access traditional passwords highlights the need for more secure means of authentication. **Two-factor authentication** increases security by validating users through a multistep process. To be authenticated, a user must provide two means of identification, one of which is typically a physical token, such as a smartcard or chip-enabled bank card, and the other of which is typically data, such as a password or personal identification number (PIN). Biometric data, such as fingerprints, iris prints, or voice prints, can also be used as one of the authenticating mechanisms. A common example of two-factor authentication is a bank card; the card itself is the physical item, and the PIN is the data that go with it.

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

FIGURE 8.4 SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2016**		**Received by: T. Benson** **Review date: June 28, 2016**	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/16	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/16	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management as well as any corrective actions management takes.

Identity Management and Authentication

Midsize and large companies have complex IT infrastructures and many systems, each with its own set of users. Identity management software automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system. It also includes tools for authenticating users, protecting user identities, and controlling access to system resources.

To gain access to a system, a user must be authorized and authenticated. **Authentication** refers to the ability to know that a person is who he or she claims to be. Authentication is often established by using **passwords** known only to authorized users. An end user uses a password to log on to a computer system and may also use passwords for accessing specific systems and files. However, users often forget passwords, share them, or choose poor passwords that are easy to guess, which compromises security. Password systems that are too rigorous hinder employee productivity. When employees must change complex passwords frequently, they often take shortcuts, such as choosing passwords that are easy to guess or keeping their passwords at their workstations in plain view. Passwords can also be sniffed if transmitted over a network or stolen through social engineering.

New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. A **token** is a physical device, similar to an identification card, that is designed to prove the identity of a single user. Tokens are small gadgets that typically fit on key rings and

chemicals used in oil and gas operations, can switch its enterprise systems from Houston to a SunGard data center in Scottsdale, Arizona, in two hours.

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

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

The Role of Auditing

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

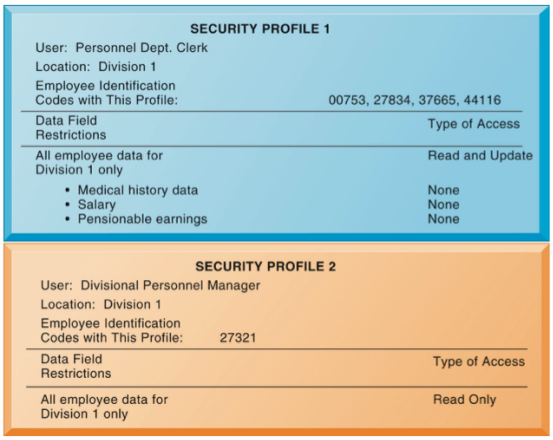
Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat. Figure 8.4 is a sample auditor's listing of control weaknesses for a loan system. It includes a section for notifying management of such weaknesses and for management's response. Management is expected to devise a plan for countering significant weaknesses in controls.

8-4 What are the most important tools and technologies for safeguarding information resources?

Businesses have an array of technologies for protecting their information resources. They include tools for managing user identities, preventing unauthorized access to systems and data, ensuring system availability, and ensuring software quality.

FIGURE 8.3 ACCESS RULES FOR A PERSONNEL SYSTEM



These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

salary, medical history, or earnings data. Another profile applies to a divisional manager, who cannot update the system but who can read all employee data fields for his or her division, including medical history and salary. We provide more detail about the technologies for user authentication later on in this chapter.

Disaster Recovery Planning and Business Continuity Planning

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

For example, MasterCard maintains a duplicate computer center in Kansas City, Missouri, to serve as an emergency backup to its primary computer center in St. Louis. Rather than build their own backup facilities, many firms contract with disaster recovery firms such as SunGard Availability Services and Acronis. These disaster recovery firms provide hot sites housing spare computers at locations around the country where subscribing firms can run their critical applications in an emergency. For example, Champion Technologies, which supplies

TABLE 8.5 ONLINE ORDER PROCESSING RISK ASSESSMENT

EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1000–$50,000 ($25,500)	$1275
User error	98%	$200–$40,000 ($20,100)	$19,698

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

Security Policy

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

The security policy drives other 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. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

Security policy also includes provisions for identity management. **Identity management** consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

Figure 8.3 is one example of how an identity management system might capture the access rules for different levels of users in the human resources function. It specifies what portions of a human resource database each user is permitted to access, based on the information required to perform that person's job. The database contains sensitive personal information such as employees' salaries, benefits, and medical histories.

The access rules illustrated here are for two sets of users. One set of users consists of all employees who perform clerical functions, such as inputting employee data into the system. All individuals with this type of profile can update the system but can neither read nor update sensitive fields, such as

(CFTC), which oversees the futures markets. This whistleblower, who declined to be identified, had spent hundreds of hours analyzing data. A new team of investigators from the U.S. Justice Department and the CFTC worked over two years to construct a case against Sarao for manipulating the market and contributing to the flash crash.

The CFTC did not blame the crash solely on Sarao, but according to the Commission's director of enforcement, Aitan Goelman, Sarao's conduct was significantly responsible for the order imbalance that led to the crash. Sarao's lawyers argued that the crash was caused by other factors and market participants. If convicted of all charges, Sarao could face a prison sentence of more than 300 years.

It is now believed that investigators overlooked evidence available hours after the flash crash that could have led them to Sarao. At that time, investigators had access to the full set of data from the day of the flash crash but focused only on the data related to actual trades. If they had included all bids and offers entered, they would have more likely noticed the pattern of Sarao's market manipulation.

After the flash crash, several reforms were implemented, including a system to slow trading in stocks if they became too volatile and a requirement for trading firms sending orders into the market to tighten their risk controls. The financial industry is also working on a consolidated audit trail, or CAT, that would enable regulators to monitor stock and options orders in real time and quickly pinpoint manipulators. CAT has yet to be completed.

Sources: Aruna Chad Bray, "Judge Orders Extradition to U.S. in 'Flash Crash' Case," *New York Times,* March 23, 2016; Aruna Viswanatha, Bradley Hope, and Chiara Albanese, "Accused Trader Accused His Rivals," *Wall Street Journal,* May 14, 2015; Aruna Viswatnatha, Bradley Hope, and Jennny Strasburg, " ' Flash Crash' Charges Filed," *Wall Street Journal,* April 21, 2015; Bradley Hope and Andrew Ackerman, "'Flash Crash' Overhaul Is Snarled in Red Tape," *Wall Street Journal,* May 5, 2015; Nathaniel Popper and Jenny Anderson, "Trader Arrested in Manipulation That Contributed to 2010 'Flash Crash,'" *New York Times,* April 21, 2015; Bradley Hope and Andrew Ackerman, "'Flash Crash' Investigators Likely Missed Clues," *Wall Street Journal,* April 26, 2015.

CASE STUDY QUESTIONS

1. Identify the problem and the control weaknesses described in this case.
2. What management, organization, and technology factors contributed to this problem? To what extent was it a technology problem? To what extent was it a management and organizational problem?
3. To what extent was Sarao responsible? Explain your answer.
4. Is there an effective solution to this problem? Can another flash crash be prevented? Explain your answer.

Table 8.5 illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an average loss calculated by adding the highest and lowest figures and dividing by two. The expected annual loss for each exposure can be determined by multiplying the average loss by its probability of occurrence.

This risk assessment shows that the probability of a power failure occurring in a one-year period is 30 percent. Loss of order transactions while power is down could range from $5000 to $200,000 (averaging $102,500) for each occurrence, depending on how long processing is halted. The probability of embezzlement occurring over a yearly period is about 5 percent, with potential losses ranging from $1000 to $50,000 (and averaging $25,500) for each occurrence. User errors have a 98 percent chance of occurring over a yearly period, with losses ranging from $200 to $40,000 (and averaging $20,100) for each occurrence.

INTERACTIVE SESSION: ORGANIZATIONS

The Flash Crash: A New Culprit

At 2:42 p.m. on May 6, 2010, U.S. stock markets suffered a trillion-dollar stock market crash lasting 26 minutes. During that brief period, the Dow Jones Industrial Average, which represents 30 of the largest American companies, plummeted more than 600 points in less than five minutes. Shares of some prominent companies such as Procter & Gamble and Accenture traded down as low as a penny or as high as $100,000. By 3:07 p.m., the market had regained nearly all the points it had lost that afternoon. Nevertheless, some were left with huge losses and others with enormous profits from this flash crash, and the confidence of the American public in the stock market was severely shaken.

How could this have happened? Several financial companies, such as Universa Investments and Waddell & Reed, had placed very large trades betting that the S&P 500 index would drop. After these trades, the market began spiraling downward as other investors rapidly followed suit, selling or making bets of their own to reduce their risk. The market was overwhelmed by sell orders with no legitimate buyers to meet those orders.

Experts initially attributed the crash to structural and organizational features of the electronic trading systems that execute the majority of trades on the Dow and the rest of the world's major stock exchanges. The huge wave of flash crash sell orders intensified because of high-speed computerized trading programs. High-frequency traders (HFTs) have taken over many of the responsibilities once filled by stock exchange specialists and market makers whose job was to provide the majority of stock market liquidity. But many electronic systems, such as those HFTs use, are automated, using algorithms to place their nearly instant trades. In situations like the flash crash, when an algorithm is insufficient to handle the complexity of the event in progress, electronic trading systems have the potential to make a bad situation much worse.

Five years later, another explanation emerged. A single trader who operated out of his West London home was largely responsible for the event. On April 21, 2015, the United States Justice Department had British authorities arrest 36-year-old Navinder Sarao, charging him with profiting from the flash crash by boldly manipulating markets and using illegal trading strategies between 2009 and 2014. Sarao was accused of having placed and withdrawn thousands of orders worth tens of millions of dollars each on hundreds of trading days to push down the price of futures contracts tied to the value of the Standard & Poor's 500 stock index. (A futures contract is an agreement to buy or sell a particular commodity or financial instrument at a predetermined price in the future.) When the price fell, Sarao would buy the contract and realize profits.

On the day of the flash crash, Sarao repeatedly placed large orders representing $170 million to more than $200 million and then canceled them just before they were executed, making the market even more vulnerable to big moves when several other investors made a big trade that day. The falling price of the futures contracts that Sarao was trading spread to related markets, triggering a cascade of trades and contributing to the Dow Jones industrial average 600-point free fall.

This technique is called *spoofing* or *layering*, and it is illegal. A trader enters large orders to buy or sell a contract to trick other traders into thinking the price is rising or falling. That trader then quickly cancels the original order and places other orders that take advantage of the price movements. The illegal strategy can be executed in fractions of a second, which makes surveillance difficult.

Authorities said Sarao had pocketed $40 million in profits from 2010 to 2014 through such manipulations, including $879,000 on the day of the flash crash. They allege that Sarao tinkered with commercially available software to create an automated trading algorithm that allowed him to place and cancel orders instantaneously. Sarao claims that he is an "old school point-and-click" trader with unusually good reflexes and intuition and that he had canceled large volumes of orders manually without the help of an automated trading program. He also noted that he had complained more than 100 times to the Chicago Mercantile Exchange, where he had traded futures contracts, about the manipulative trading practices of other HFTs.

Long before the flash crash, the exchange had questioned Sarao about his trading activity, but the exchange did not take any action against him, and Sarao continued his trading activities until April 2015. Finally, a whistleblower brought new information to the Commodity Futures Trading Commission

TABLE 8.4 GENERAL CONTROLS

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

Information systems controls should not be an afterthought. They need to be incorporated into the design of a system and should consider not only how the system will perform under all possible conditions but also the behavior of organizations and people using the system. The Interactive Session on Organizations describes control weaknesses in systems that many organizations and people use for electronic trading and the role they played in the 2010 flash crash.

Risk Assessment

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

A **risk assessment** determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. For example, if an event is likely to occur no more than once a year, with a maximum of a $1000 loss to the organization, it is not wise to spend $20,000 on the design and maintenance of a control to protect against that event. However, if that same event could occur at least once a day, with a potential loss of more than $300,000 a year, $100,000 spent on a control might be entirely appropriate.

- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

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

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

8-3 What are the components of an organizational framework for security and control?

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

Information Systems Controls

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

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems development process, and administrative controls. Table 8.4 describes the functions of each of these controls.

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

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

If you work in a firm providing financial services, your firm will need to comply with the Financial Services Modernization Act of 1999, better known as the **Gramm-Leach-Bliley Act** after its congressional sponsors. This act requires financial institutions to ensure the security and confidentiality of customer data. Data must be stored on a secure medium, and special security measures must be enforced to protect such data on storage media and during transmittal.

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

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

Electronic Evidence and Computer Forensics

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

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

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

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data

very little time to respond between the time a vulnerability and a patch are announced and the time malicious software appears to exploit the vulnerability.

8-2 What is the business value of security and control?

Companies have very valuable information assets to protect. Systems often house confidential information about individuals' taxes, financial assets, medical records, and job performance reviews. They also can contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. Government systems may store information on weapons systems, intelligence operations, and military targets. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands. Systems that are unable to function because of security breaches, disasters, or malfunctioning technology can have permanent impacts on a company's financial health. Some experts believe that 40 percent of all businesses will not recover from application or data losses that are not repaired within three days.

Inadequate security and control may result in serious legal liability. Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Failure to do so may open the firm to costly litigation for data exposure or theft. An organization can be held liable for needless risk and harm created if the organization fails to take appropriate protective action to prevent loss of confidential information, data corruption, or breach of privacy. For example, Target had to pay $39 million to several U.S. banks servicing Mastercard that were forced to reimburse Target customers millions of dollars when those customers lost money due to a massive 2013 hack of Target's payment systems affecting 40 million people. Target also paid $67 million to Visa for the data hack and $10 million to settle a class-action lawsuit brought by Target customers. A sound security and control framework that protects business information assets can thus produce a high return on investment. Strong security and control also increase employee productivity and lower operational costs.

Legal and Regulatory Requirements for Electronic Records Management

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

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

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

Software Vulnerability

Software errors pose a constant threat to information systems, causing untold losses in productivity and sometimes endangering people who use or depend on systems. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities. On April 29, 2015, American Airlines had to delay 40 flights due to faulty software on iPads pilots use to look at airport maps and navigational documents. The problem was fixed by having the pilots delete the malfunctioning app and reinstall it (Bajaj, 2015).

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

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

Flaws in commercial software not only impede performance but also create security vulnerabilities that open networks to intruders. Each year security firms identify thousands of software vulnerabilities in Internet and PC software. A recent example is the Heartbleed bug, which is a flaw in OpenSSL, an open-source encryption technology that an estimated two-thirds of web servers use. Hackers could exploit the bug to access visitors' personal data as well as a site's encryption keys, which can be used to collect even more protected data.

Especially troublesome are **zero-day vulnerabilities**, which are holes in the software unknown to its creator. Hackers then exploit this security hole before the vendor becomes aware of the problem and hurries to fix it. This type of vulnerability is called zero day because the author of the software has zero days after learning about it to patch the code before it can be exploited in an attack. Sometimes security researchers spot the software holes but, more often, they remain undetected until an attack has occurred.

To correct software flaws once they are identified, the software vendor creates small pieces of software called **patches** to repair the flaws without disturbing the proper operation of the software. It is up to users of the software to track these vulnerabilities, test, and apply all patches. This process is called *patch management*.

Because a company's IT infrastructure is typically laden with multiple business applications, operating system installations, and other system services, maintaining patches on all devices and services a company uses is often time-consuming and costly. Malware is being created so rapidly that companies have

Global Threats: Cyberterrorism and Cyberwarfare

The cyber criminal activities we have described—launching malware, DoS attacks, and phishing probes—are borderless. Attack servers for malware are now hosted in more than 200 countries and territories. The most popular sources of malware attacks include the United States, India, Germany, South Korea, China, Netherlands, United Kingdom, and Russia. The global nature of the Internet makes it possible for cybercriminals to operate—and to do harm—anywhere in the world.

Internet vulnerabilities have also turned individuals and even entire nation-states into easy targets for politically motivated hacking to conduct sabotage and espionage. **Cyberwarfare** is a state-sponsored activity designed to cripple and defeat another state or nation by penetrating its computers or networks to cause damage and disruption. Cyberwarfare also includes defending against these types of attacks.

Cyberwarfare is more complex than conventional warfare. Although many potential targets are military, a country's power grids, financial systems, and communications networks can also be crippled. Non-state actors such as terrorists or criminal groups can mount attacks, and it is often difficult to tell who is responsible. Nations must constantly be on the alert for new malware and other technologies that could be used against them, and some of these technologies developed by skilled hacker groups are openly for sale to interested governments.

Preparations for cyberwarfare attacks have become much more widespread, sophisticated, and potentially devastating. Between 2011 and 2015, foreign hackers stole source code and blueprints to the oil and water pipelines and power grid of the United States and infiltrated the Department of Energy's networks 150 times (Perlroth, 2015). Over the years, hackers have stolen plans for missile tracking systems, satellite navigation devices, surveillance drones, and leading-edge jet fighters.

A 2015 report documented 29 countries with formal military and intelligence units dedicated to offensive cyberwarfare. Their cyberarsenals include collections of malware for penetrating industrial, military, and critical civilian infrastructure controllers, e-mail lists and text for phishing attacks on important targets, and algorithms for DoS attacks. U.S. cyberwarfare efforts are concentrated in the United States Cyber Command, which coordinates and directs the operations and defense of Department of Defense information networks and prepares for military cyberspace operations. Cyberwarfare poses a serious threat to the infrastructure of modern societies, since their major financial, health, government, and industrial institutions rely on the Internet for daily operations.

Internal Threats: Employees

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

Studies have found that user lack of knowledge is the single greatest cause of network security breaches. Many employees forget their passwords to access computer systems or allow 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. This practice is called **social engineering**.

TABLE 8.3 MAJOR DATA BREACHES

DATA BREACH	DESCRIPTION
Anthem Health Insurance	In February 2015 hackers stole the personal information on more than 80 million customers of the giant health insurer, including names, birthdays, medical IDs, social security numbers, and income data. No medical or credit information was stolen. This was the largest healthcare breach ever recorded
Sony	In November 2014 hackers stole more than 100 terabytes of corporate data, including trade secrets, e-mail, personnel records, and copies of films for future release. Malware erased data from Sony's corporate systems, leading to hundreds of millions of dollars in losses as well as a tarnished brand image. Sony was hacked earlier in April 2011 when intruders obtained personal information, including credit, debit, and bank account numbers, from more than 100 million PlayStation Network users and Sony Online Entertainment users.
Home Depot	Hacked in 2014 with a malicious software program that plundered store registers while disguising itself as antivirus software. Fifty-six million credit card accounts were compromised, and 53 million customer e-mail addresses were stolen.
Target	Malware surreptitiously installed on security and payment systems in late 2013 stole credit card numbers and identifying data for 40 million Target customers and e-mail addresses of 70 million customers.
eBay	Cyberattack on eBay servers during February and March 2014 compromised database containing customer names, encrypted passwords, e-mail addresses, physical addresses, phone numbers, and birthdates; 145 million people were affected.

U.S. legislation, such as the Wiretap Act, Wire Fraud Act, Economic Espionage Act, Electronic Communications Privacy Act, CAN-SPAM Act, and Protect Act of 2003 (prohibiting child pornograpy), covers computer crimes involving intercepting electronic communication, using electronic communication to defraud, stealing trade secrets, illegally accessing stored electronic communications, using e-mail for threats or harassment, and transmitting or possessing child pornography. A proposed federal Data Security and Breach Notification Act would mandate organizations that possess personal information to put in place "reasonable" security procedures to keep the data secure and notify anyone affected by a data breach, but it has not been enacted.

Click Fraud

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

Some companies hire third parties (typically from low-wage countries) to click a competitor's ads fraudulently to weaken them by driving up their marketing costs. Click fraud can also be perpetrated with software programs doing the clicking, and botnets are often used for this purpose. Search engines such as Google attempt to monitor click fraud and have made some changes to curb it.

companies are reluctant to report computer crimes because the crimes may involve employees, or the company fears that publicizing its vulnerability will hurt its reputation. The most economically damaging kinds of computer crime are DoS attacks, activities of malicious insiders, and web-based attacks.

Identity Theft

With the growth of the Internet and electronic commerce, identity theft has become especially troubling. **Identity theft** is a crime in which an imposter obtains key pieces of personal information, such as social security numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

Identity theft has flourished on the Internet, with credit card files a major target of website hackers. According to the 2016 Identity Fraud Study by Javelin Strategy & Research, 13.1 million consumers lost $15 billion to identity fraud in 2015 (Javelin, 2016). E-commerce sites are wonderful sources of customer personal information—name, address, and phone number. Armed with this information, criminals can assume new identities and establish new credit for their own purposes.

One increasingly popular tactic is a form of spoofing called **phishing**. Phishing involves setting up fake websites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data. The e-mail message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering the information at a bogus website, or by calling a telephone number. eBay, PayPal, Amazon.com, Walmart, and a variety of banks have been among the top spoofed companies. In a more targeted form of phishing called *spear phishing*, messages appear to come from a trusted source, such as an individual within the recipient's own company or a friend.

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

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

According to the Ponemon Institute's 2015 Cost of a Data Breach Study, the average cost of a breach to a company was $3.5 million (Ponemon, 2015). Moreover, brand damage can be significant, albeit hard to quantify. In addition to the data breaches described in the opening and ending case studies for this chapter, Table 8.3 describes other major data breaches.

The U.S. Congress addressed the threat of computer crime in 1986 with the Computer Fraud and Abuse Act, which makes it illegal to access a computer system without authorization. Most states have similar laws, and nations in Europe have comparable legislation. Congress passed the National Information Infrastructure Protection Act in 1996 to make malware distribution and hacker attacks to disable websites federal crimes.

with bot malware that opens a back door through which an attacker can give instructions. The infected computer then becomes a slave, or zombie, serving a master computer belonging to someone else. When hackers infect enough computers, they can use the amassed resources of the botnet to launch DDoS attacks, phishing campaigns, or unsolicited spam e-mail.

Ninety percent of the world's spam and 80 percent of the world's malware are delivered by botnets. For example, a new version of the Pushdo spamming botnet was detected in spring 2015. Computers in more than 50 countries were infected. Pushdo has existed since 2007 despite numerous attempts to shut it down. The latest version has been pushing malware that steals login credentials and accesses online banking systems. At one time, Pushdo-infected computers sent as many as 7.7 billion spam messages per day (Kirk, 2015).

Computer Crime

Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of **computer crime** as well. Computer crime is defined by the U.S. Department of Justice as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." Table 8.2 provides examples of the computer as both a target and an instrument of crime. The chapter-opening case describes one of the largest financial computer crime cases reported to date.

No one knows the magnitude of the computer crime problem—how many systems are invaded, how many people engage in the practice, or the total economic damage. According to the Ponemon Institute's 2015 Annual Cost of Cyber Crime Study, the average annualized cost of cybercrime for U.S. companies benchmarked was $15 million per year (Ponemon Institute, 2015). Many

TABLE 8.2 EXAMPLES OF COMPUTER CRIME

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

Hackers and Computer Crime

A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term *cracker* is typically used to denote a hacker with criminal intent, although in the public press, the terms *hacker* and *cracker* are used interchangeably. Hackers gain unauthorized access by finding weaknesses in the security protections websites and computer systems employ, often taking advantage of various features of the Internet that make it an open system and easy to use. Hacker activities have broadened beyond mere system intrusion to include theft of goods and information as well as system damage and **cybervandalism**, the intentional disruption, defacement, or even destruction of a website or corporate information system.

Spoofing and Sniffing

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

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

Denial-of-Service Attacks

In a **denial-of-service (DoS) attack**, hackers flood a network server or web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A **distributed denial-of-service (DDoS)** attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a website to shut down, making it impossible for legitimate users to access the site. For example, on April 27, 2015, the state of Hawaii and the Thirty Meter Telescope (TMT) were hit with a DoS attack believed to have been launched by a group called Operation Green Rights. (The TMT organization is constructing one of the biggest telescopes in the world in Hawaii.) Both organizations' websites were flooded with so much illicit traffic that they were not available until the following day (Wakida, 2015).

For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. Especially vulnerable are small and midsize businesses whose networks tend to be less protected than those of large corporations.

Perpetrators of DDoS attacks often use thousands of zombie PCs infected with malicious software without their owners' knowledge and organized into a **botnet**. Hackers create these botnets by infecting other people's computers

IoT devices themselves, their platforms and operating systems, their communications, and even the systems to which they're connected. Additional security tools will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as attacks that drain batteries. Many IoT devices such as sensors have simple processors and operating systems that may not support sophisticated security approaches.

Panda Security reported that it had identified and neutralized more than 84 million new malware samples throughout 2015 and that it had detected 230,000 new malware samples each day. More than 27 percent of all malware samples ever recorded were created in that one year alone (Panda Security, 2016).

More than 51 percent of the infections Panda found were Trojan horses. A **Trojan horse** is a software program that appears to be benign but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system. The term *Trojan horse* is based on the huge wooden horse the Greeks used to trick the Trojans into opening the gates to their fortified city during the Trojan War. Once inside the city walls, Greek soldiers hidden in the horse revealed themselves and captured the city.

An example of a modern-day Trojan horse is the Zeus Trojan. It is often used to steal login credentials for banking by surreptitiously capturing people's keystrokes as they use their computers. Zeus is spread mainly through drive-by downloads and phishing, and recent variants are hard for anti-malware tools to detect.

SQL injection attacks have become a major malware threat. SQL injection attacks take advantage of vulnerabilities in poorly coded web application software to introduce malicious program code into a company's systems and networks. These vulnerabilities occur when a web application fails to validate properly or filter data a user enters on a web page, which might occur when ordering something online. An attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQL injection attack.

Malware known as **ransomware** is proliferating on both desktop and mobile devices. Ransomware tries to extort money from users by taking control of their computers or displaying annoying pop-up messages. One nasty example, CryptoLocker, encrypts an infected computer's files, forcing users to pay hundreds of dollars to regain access. You can get ransomware from downloading an infected attachment, clicking a link inside an e-mail, or visiting the wrong website.

Some types of **spyware** also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user web-surfing activity and serve up advertising. Thousands of forms of spyware have been documented.

Many users find such spyware annoying, and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious. **Keyloggers** 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 or bank account numbers. The Zeus Trojan described earlier uses keylogging. Other spyware programs reset web browser home pages, redirect search requests, or slow performance by taking up too much memory.

TABLE 8.1 EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Cryptolocker	Ransomware/ Trojan	Hijacks users' photos, videos, and text documents; encrypts them with virtually unbreakable asymmetric encryption; and demands ransom payment for them
Conficker	Worm	First detected in November 2008 and still a problem. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Had more than 5 million computers worldwide under its control. Difficult to eradicate.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot and infected computers to search for more victims. Affected millions of computers worldwide and caused an estimated $14.8 billion to $18.6 billion in damages.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.

machines. Especially prevalent today are **drive-by downloads**, consisting of malware that comes with a downloaded file that a user intentionally or unintentionally requests.

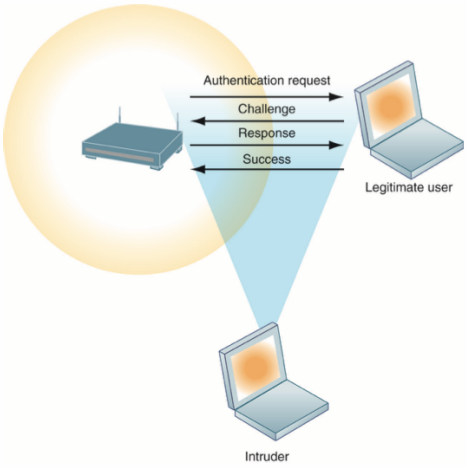
Hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background to monitor user actions, and potentially convert the smartphone to a robot in a botnet to send e-mail and text messages to anyone. With smartphones outselling PCs and increasingly used as payment devices, they are becoming a major avenue for malware.

According to IT security experts, mobile devices now pose the greatest security risks, outpacing those from larger computers. By the end of 2015, McAfee Labs had collected more than 6 million samples of mobile malware (Snell, 2016). Android, which is the world's leading mobile operating system, is the platform targeted by most hackers. Mobile device viruses pose serious threats to enterprise computing because so many wireless devices are now linked to corporate information systems (see the Interactive Session on Technology in Section 8-4).

Blogs, wikis, and social networking sites such as Facebook, Twitter, and LinkedIn have emerged as new conduits for malware. Members are more likely to trust messages they receive from friends, even if this communication is not legitimate. One malware scam in spring 2015 appeared to be a video link from a friend saying something like, "This is awesome." If the recipient clicked the link. a pop-up window appeared and prompted that person to click an Adobe Flash Player update to continue. Instead of downloading the player, the malware took over the user's computer, looking for bank account numbers, medical records, and other personal data (Thompson, 2015).

Security risks are bound to increase from the mushrooming number of Internet-linked devices within companies and across the Internet. The Internet of Things (IoT) introduces a wide range of new security challenges to

FIGURE 8.2 WI-FI SECURITY CHALLENGES



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

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

Malicious software programs are referred to as **malware** and include a variety of threats such as computer viruses, worms, and Trojan horses. (See Table 8.1.) A **computer virus** is a rogue software program that attaches itself to other software programs or data files to be executed, usually without user knowledge or permission. Most computer viruses deliver a payload. The payload may be relatively benign, such as instructions to display a message or image, or it may be highly destructive—destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly. Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file.

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

Worms and viruses are often spread over the Internet from files of downloaded software; from files attached to e-mail transmissions; or from compromised e-mail messages, online ads, or instant messaging. Viruses have also invaded computerized information systems from infected disks or infected

Internet Vulnerabilities

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

Telephone service based on Internet technology (see Chapter 7) is more vulnerable than the switched voice network if it does not run over a secure private network. Most Voice over IP (VoIP) traffic over the Internet is not encrypted. Hackers can intercept conversations or shut down voice service by flooding servers supporting VoIP with bogus traffic.

Vulnerability has also increased from widespread use of e-mail, instant messaging (IM), and peer-to-peer (P2P) file-sharing programs. E-mail may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients. Popular IM applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by outsiders during transmission over the Internet. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network. Sharing files over P2P networks, such as those for illegal music sharing, may also transmit malicious software or expose information on either individual or corporate computers to outsiders.

Wireless Security Challenges

Is it safe to log on to a wireless network at an airport, library, or other public location? It depends on how vigilant you are. Even the wireless network in your home is vulnerable because radio frequency bands are easy to scan. Both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers. Local area networks (LANs) using the 802.11 standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic, and, in some cases, gain access to the Internet or to corporate networks.

Wi-Fi transmission technology was designed to make it easy for stations to find and hear one another. The service set identifiers (SSIDs) that identify the access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by intruders' sniffer programs (see Figure 8.2). Wireless networks in many locations do not have basic protections against **war driving**, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

An intruder who has associated with an access point by using the correct SSID is capable of accessing other resources on the network. For example, the intruder could use the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files.

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

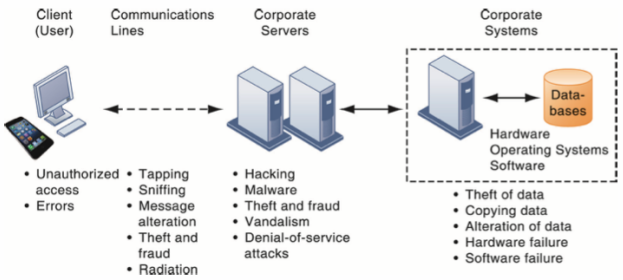
access, abuse, or fraud is not limited to a single location but can occur at any access point in the network. Figure 8.1 illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multitier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter data without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-of-service attacks or malicious software to disrupt the operation of websites. Those capable of penetrating corporate systems can steal, destroy, or alter corporate data stored in databases or files.

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

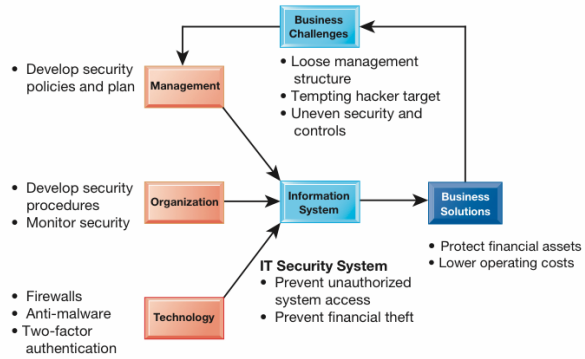
Domestic or offshore partnering with another company contributes to system vulnerability if valuable information resides on networks and computers outside the organization's control. Without strong safeguards, valuable data could be lost, destroyed, or fall into the wrong hands, revealing important trade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

The popularity of handheld mobile devices for business computing adds to these woes. Portability makes cell phones, smartphones, and tablet computers easy to lose or steal. Smartphones share the same security weaknesses as other Internet devices and are vulnerable to malicious software and penetration from outsiders. Smartphones that corporate employees use often contain sensitive data such as sales figures, customer names, phone numbers, and e-mail addresses. Intruders may also be able to access internal corporate systems through these devices.

FIGURE 8.1 CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES



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



instructions over the SWIFT system to illicitly transfer funds to their accounts. SWIFT is now working with member institutions to upgrade their security, but it will take years before all participants in the network are fully protected.

Here are some questions to think about: What security vulnerabilities were exploited by the hackers? What management, organizational, and technological factors contributed to these security weaknesses? What was the business impact of these problems?

8-1 Why are information systems vulnerable to destruction, error, and abuse?

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

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

Why Systems are Vulnerable

When large amounts of data are stored in electronic form, they are vulnerable to many kinds of threats. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized

How could this have happened? SWIFT isn't regulated like a bank because it doesn't hold funds or manage accounts. It's overseen by the National Bank of Belgium and representatives from the U.S. Federal Reserve, the Bank of England, the European Central Bank, the Bank of Japan, and other major banks. Experts point out that the SWIFT system is based on flexibility and trust. A bank can choose to let employees open SWIFT's main interface right from their desktop browser. That same feature that makes SWIFT easy to use also makes the system susceptible to hacking. Hackers apparently were able to obtain the banks' SWIFT access codes, send authenticated but fraudulent requests to transfer funds, and cover their tracks with malware surreptitiously placed onto bank computer systems. These attacks showed a deep and sophisticated knowledge of specific controls at the targeted banks, which may have been acquired from insiders, cyberattacks, or both.

Most banks in the United States take special precautions with their SWIFT-linked computers, including multiple firewalls to isolate SWIFT from the bank's other networks and even operating the machines in separate locked rooms. Unfortunately some banks in other countries take fewer precautions. The Bangladesh bank may have been especially vulnerable, using $10 routers and no firewalls, according to experts.

Security firms and intelligence agencies are still trying to learn who is behind the attacks. Symantec Corp, a leading security company, says the attacks resemble earlier hacking efforts attributed to North Korea.

SWIFT plans to toughen software requirements, expand the use of two-factor authentication (which provides additional identity checking), monitor compliance more rigorously, and provide more information about fraud detection. Ultimately, however, SWIFT can only do so much. The real solution must come from the participating banks themselves. And according to SWIFT CEO Gottfried Leibbrandt, fully armoring the network's defenses is likely to take years.

Sources: Michael Corkery, "Hackers' $81 Million Sneak Attack on World Banking," *New York Times*, April 30, 2016; Katy Burne, Robin Sidel, and Syed Zain Al-Mahmood, "Swift Banking Network Struggles with Wave of Cyberattacks," *Wall Street Journal*, May 20, 2016; "What a Bank Heist Reveals About Global Security," *Bloomberg View*, May 31, 2016; John Detrixhe, Gavin Finch, and John Follain, "Swift CEO Expects More Hacking Surprises as Fix Is Years Away," *Bloomberg Business Week*, June 2, 2016.

The problems created by the $81 million theft resulting from break-ins to the SWIFT global banking network illustrate some of the reasons businesses need to pay special attention to information system security. The SWIFT system is a critical tool for global business. But from a security standpoint, as this case illustrates, the system was vulnerable to hackers who were able to access supposedly protected user authentication data.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. The SWIFT system is flexible and easy to use and does not require the same high level of security among its participating institutions. Although major banks in the United States using the SWIFT network have strong information system security in place, the security used by other SWIFT network members for protecting global banking transactions was weak. Despite the strong security safeguards of the SWIFT network itself, criminals were able to break into the systems of SWIFT member banks and send false

Hackers Attack the SWIFT Global Banking Network

SWIFT, which stands for Society for Worldwide Interbank Financial Telecommunication, is considered the Rolls-Royce of payment networks. It is a system used by more than 11,000 financial institutions worldwide to authorize payments from one account to another. SWIFT's secure messaging system sends about 25 million messages on a typical day, including orders and confirmations for payments, securities settlements, and currency exchanges. Obviously, this is a very important system for global finance. If you receive a message from SWIFT, you can be sure it's legitimate and move the money as expected.

© Brian Jackson/123RF

SWIFT is a highly secure system, but apparently not secure enough. In early 2016 revelations surfaced about multiple attempts to use SWIFT messaging to rob financial institutions. Bangladesh's central bank disclosed that in February 2016 it had lost $81 million to hackers who breached its security, accessed SWIFT, and tricked the Federal Reserve Bank of New York into sending funds it held for the bank to hacker-controlled accounts in the Philippines.

Each bank in the SWIFT network is identified by a set of codes. Hackers somehow managed to steal the Bangladesh bank's credentials to transmit the messages and used malware targeting a PDF reader for checking statements. SWIFT's core messaging system was not compromised. Security breaches occurred in the computers of individual institutions that interact with the system, and these computers remain the responsibility of individual SWIFT members. The hackers had access only to the compromised banks' funds but not to the funds of the thousands of other institutions that use SWIFT. However, investigators have identified breaches at 12 other banks, including Vietnam's Tien Phong Commercial Joint Stock Bank and Ecuador's Banco del Austro.

CHAPTER 8

Securing Information Systems

Learning Objectives

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

- **8-1** Why are information systems vulnerable to destruction, error, and abuse?
- **8-2** What is the business value of security and control?
- **8-3** What are the components of an organizational framework for security and control?
- **8-4** What are the most important tools and technologies for safeguarding information resources?

MyMISLab™

Visit **mymislab.com** for simulations, tutorials, and end-of-chapter problems.

CHAPTER CASES

Hackers Attack the SWIFT Global Banking Network
The Flash Crash: A New Culprit
BYOD: A Security Nightmare?
U.S. Office of Personnel Management Data Breach: No Routine Hack

VIDEO CASES

Stuxnet and Cyberwarfare
Cyberespionage: The Chinese Threat
Instructional Videos:
Sony PlayStation Hacked; Data Stolen from 77 Million Users
Meet the Hackers: Anonymous Statement on Hacking Sony