Chapter 5

IT Security, Crime, Compliance, and Continuity

Learning Objectives

1. Understand the objectives, functions, and financial value of IT security.
2. Recognize IS vulnerabilities, threats, attack methods, and cybercrime symptoms.
3. Understand crimes committed against computers and crimes committed with computers.
4. Explain key methods of defending information systems, networks, and wireless devices.
5. Understand network security risks and defenses.
6. Describe internal control and fraud and the related legislation.
7. Understand business continuity and disaster recovery planning methods.

Integrating *IT*

CHAPTER 5 LINK LIBRARY

Information Security Magazine *searchsecurity.techtarget.com/*
CIO Magazine, IT Security *cio.com/topic/3089/Security*
Computer and Internet Security *cnet.com/internet-security*
IT Governance Institute *itgi.org*
U.S. Computer Emergency Readiness Team (US-CERT) *us-cert.gov/cas/tips/*
SANS Information Security Reading Room *sans.org/reading_room/*
Privacy news from around the world *pogowasright.org/*
Government Computer News (GCN) *gcn.com/*
CompTIA *comptia.org/*
F-Secure *f-secure.com/en_US/security/security-center/*
Social engineering *symantec.com/connect/articles/social-engineering*

QUICK LOOK at Chapter 5, IT Security, Crime, Compliance, and Continuity

This section introduces you to the business issues, challenges, and IT solutions in Chapter 5. Topics and issues mentioned in the Quick Look are explained in the chapter.

Information security (*infosec*, for short) is about risk to data, information systems, and networks. These incidents create business and legal risks, such as when operations are disrupted or privacy laws are violated.

IT risk management includes securing corporate systems while ensuring their availability; planning for disaster recovery and business continuity; complying with government regulations and license agreements; maintaining internal controls; and protecting the organization against an increasing array of threats such as viruses, worms, spyware, and other forms of malware. In general, risk management is both expensive and inconvenient. Many users, for instance, complain about being forced to use strong passwords (i.e., at least 10 characters and must contain a digit and special character) that aren't easy to remember.

Managers have a **fiduciary responsibility** (legal and ethical obligation) to protect the confidential data of the people and partners that they collect, store, and share. To comply with international, federal, state, and foreign laws, companies must invest in IT security to protect their data, other assets, the ability to operate, and net income. Losses and disruptions due to IT security breaches can seriously harm or destroy a company both financially and operationally. As the effectiveness of the technology and tactics used by **cybercriminals**—people who commit crimes using the Internet—increases, so do the costs (and inconveniences) of staying ahead of deliberate attacks, viruses and other malware infections, and unintentional errors.

In this chapter we begin with an overview of enterprise-wide security issues. We discuss technologies, such as firewalls and malware, internal controls, information assurance, and the enterprise risk management (ERM) and COBIT framework. We base infosec on a risk exposure model for identifying what to protect and how much to invest in that protection.

Swiss Bank Account Data Stolen from HSBC Private Bank

In March 2010, HSBC admitted to the theft of confidential account data of 24,000 clients, or 15 percent, of its Private Bank in Switzerland. Account information was stored securely in encrypted files, but those files were carried out of the bank on a laptop by Herve Falciani, a former IT specialist based in HSBC's Geneva branch. In April 2010, French prosecutor Eric

de Montgolfier said that when the stolen files were decrypted, investigators identified 127,000 accounts belonging to 79,000 clients—more than triple HSBC's estimate.

Ironically, Falciani allegedly stole the files in 2007 during a project to transfer information to a more secure system.

Impact of Data Exposure on Clients

HSBC had no idea that their data had been stolen until after Falciani tried to sell it to the French authorities, who arrested him. The criminal investigation of Falciani is being conducted by the Swiss federal prosecutor.

In January 2009, French police obtained the evidence—the encrypted files—after raiding Falciani's home in France. While the information may not have been sold to identity thieves or other criminals, the clients whose data was stolen may be facing legal problems in their own countries.

- **France:** Authorities in France are seeking to track down clients who hide assets in HSBC's private bank and to investigate suspected tax evasion by wealthy French taxpayers.
- **Italy:** Italian authorities are interested in the data for similar investigations into tax evasion and money laundering.
- **Germany:** According to the German newspaper *Der Spiegel*, Falciani had also tried to sell details of 3,000 accounts and 1,300 names of German taxpayers to the German authorities for 2.5 million euros. The estimated tax recovery would be between 100 and 200 million euros. German Finance Minister Wolfgang Schaeuble said he would buy the data, which led to a public outcry: *How dare Germany seek to profit from an illegal act.*

Impact of Insider Data Theft on HSBC Private Bank

HSBC invested an additional $93 million to upgrade its computer systems and data security procedures after the breach. However, that may be the lowest cost impact. The privacy invasion and legal exposure clients faced because of the data breach may be devastating to the reputation of HSBC Private Bank in Switzerland (*hsbcprivatebank.com/*)—given several of the reasons for such private accounts.

Alexandre Zeller, CEO of HSBC Private Bank in Switzerland, apologized to clients, saying; "We deeply regret the situation and unreservedly apologize to our clients for this threat to their privacy." To help reassure clients, HSBC said it would refuse to help authorities use the stolen data for tax evasion investigations.

Inadequate security controls have cost HSBC more than just its reputation. HSBC faced very expensive legal problems. Swiss regulators were investigating whether HSBC broke the country's strict bank privacy laws, which carries severe penalties.

Sources: Compiled from Barrett (2010), HSBC-RI (2010), Leyden (2010).

For Class Discussion and Debate

1. ***Scenario for Brainstorming and Discussion:*** Complete (100%) security is impossible. Therefore, companies must decide how much to invest in infosec policies, procedures, and training as well as the enforcement of those policies and procedures. Discuss why senior management commitment and support are important to infosec. Brainstorm ways to determine how much to invest in infosec. Assume that a company's budget is fixed. Therefore, investment in infosec reduces funds available for other functions, such as marketing, new product development, and so on.

2. ***Debate:*** This incident has raised difficult questions about privacy and the ethics of how far authorities or law enforcement should be allowed to go to identify suspected tax dodgers, money launderers, or other types of criminals. Money laundering is known to be widely used to fund or support terrorism. Therefore, any investigation into money laundering may be in the public's best interests but an invasion of someone's privacy. Another perspective is best represented by the outcry *how dare Germany seek to profit from an illegal act.*

Is it ethical for authorities to use the private data that Falciani had stolen as evidence to investigate tax evasion and money laundering?

- If *yes,* then should there be any restrictions on the use of that data?
- If *no,* then if the public's safety or security was at potential risk, should the privacy of the clients' stolen data be allowed as evidence?

To Do: Select one side of the argument—either *in favor of privacy* or *in favor of public security,* as just described. Debate the ethical issues associated with your side of the argument.

5.1 Protecting Data and Business Operations

What is information and network security? Most people would mention hardware and software in their answers; for example, firewalls, encryption, antivirus, antispam, anti-spyware, anti-phishing, and so on. Firewalls and intrusion detection systems are placed throughout networks to monitor and control traffic into and out of a network, as shown in Figure 5.1.

Certainly, technology defenses are necessary, but they're insufficient because protecting data and business operations involves all of the following:

- Making data and documents available and accessible 24/7 while simultaneously restricting access
- Implementing and enforcing procedures and acceptable use policies for company-owned data, hardware, software, and networks
- Promoting secure and legal sharing of information among authorized persons and partners
- Ensuring compliance with government regulations and laws
- Preventing attacks by having network intrusion defenses in place
- Detecting, diagnosing, and reacting to incidents and attacks in real time
- Maintaining internal controls to prevent manipulation of data and records
- Recovering from business disasters and disruptions quickly

As the prior list shows, business policies, procedures, training, and disaster recovery plans as well as technology all play a critical role in IT security. **IT security** covers the protection of information, communication networks, and traditional and e-commerce operations to assure their confidentiality, integrity, availability, and authorized use.

Until 2002, infosec was mostly a technology issue assigned to the IT department. Incidents were handled on a case-by-case "cleanup" basis rather than by taking a preemptive approach to protect ahead of the threats. Infosec was viewed as a *cost* rather than as a *resource* for preventing business disruptions and satisfying governance responsibilities. The cost-based view turned out to be dangerously inadequate at securing the enterprise against dishonest insiders and the global reach of cybercrimes, malware, spyware, and fraud.

During 2010, hi-tech criminals were launching more than 100 attacks per second on computers worldwide, according to a report from IT security vendor Symantec. While most of these attacks didn't cause trouble, one attack every 4.5 seconds did affect a PC. Symantec identified almost 2.9 million items of malicious code during a 12-month period. The steep rise in malware was driven largely by the availability of free, easy-to-use, and/or powerful toolkits that novice cybercriminals were using to develop their own malware. For example, one malware toolkit named Zeus cost $700 (£458), and many had become so successful that their creators offered telephone

Figure 5.1 Firewalls protect networks by controlling incoming and outgoing traffic. (*GodfriedEdelman/iStockphoto*)

support for those who could not get their worms or viruses to work. Cleanup costs after a single incident are already into the hundreds of millions of dollars.

KNOW YOUR ENEMY AND YOUR RISKS

Every enterprise has information that profit-motivated criminals (who may be across the globe or may be trusted employees) want to, and may actually attempt to, steal and/or sell. The opening case about HSBC Private Bank demonstrates why IT security risks are business risks. Those risks can stem from insiders, outsiders, cybercriminal organizations, or malware. **Malware** is short for *malicious software,* referring to viruses, worms, Trojan horses, spyware, and all other types of disruptive, destructive, or unwanted programs. Threats range from high-tech exploits to gain access to a company's networks and databases to nontech tactics to steal laptops and whatever else is available. Because infosec terms, such as *threats* and *exploits*, have precise meanings, the key terms and their meanings are listed in Table 5.1.

In general, IT security measures have focused on protecting against outsiders and malware. While controlling physical and remote access to databases and networks is still challenging, a majority of data breaches involve some sort of insider error or action—either intentional or unintentional. That is, the greatest infosec risks are employees and managers. Companies suffer tremendous loss from fraud committed by employees. It's a widespread problem that affects every company, regardless of size, location, or industry. You will read more about fraud in Section 5.3.

IT security is so integral to business objectives that it cannot be treated as a stand-alone function. Failures have a direct impact on business performance, customers, business partners, and stakeholders—and can lead to fines, legal action, and steep declines in stock prices as investors react to the crisis.

Internal Threats: Employees Threats from employees, referred to as **internal threats,** are a major challenge largely due to the many ways an employee can carry out malicious activity. Insiders may be able to bypass physical security (e.g., locked doors) and technical security (e.g., passwords) measures that organizations have in place to prevent unauthorized access. Why? Because defenses such as firewalls, intrusion detection systems (IDS), and locked doors mostly protect against external threats. As you have read, incidents that cause the greatest damages or losses are those carried out by insiders. Despite the challenges, insider incidents can be minimized with a layered defense strategy consisting of security procedures, acceptable use policies, and technology controls.

The following incidents, all of which were caused by insiders, could have been prevented if strict infosec policies and defenses had been enforced.

- In April 2010, Thomas A. Drake, a former high-ranking National Security Agency (NSA) official, was indicted for having used a secret, nongovernment e-mail account to transmit classified information that he was not authorized to access or disclose. The indictment alleged that in early 2006, Drake signed up for an account with Hushmail, which provides encrypted e-mail. He had contacted a reporter for a national newspaper, who also signed up for Hushmail, enabling them to exchange secret government documents. The reporter published reports about the NSA that contained classified Signals Intelligence information, which involves collection and analysis of foreign communications (Aftergood, 2010).
- Three HSBC business units were fined more than £3.2 million by the Financial Services Authority (FSA) for security failings that led to the loss of customers' sensitive personal details, exposing them to risk of identity theft and fraud. The FSA said that HSBC customer data had been lost twice in the mail. In 2007, HSBC actuaries lost an unencrypted disk in the mail with the personal details of 2,000 pension members, including birth dates, addresses, and insurance details. Despite apologies and a warning to staff from the bank about the need for effective security procedures, another unencrypted disk was lost in the mail in 2009 by HSBC Life, containing the personal details of 180,000 policyholders.

TABLE 5.1 IT Security Terms

Term	Definition
Threat	Something or someone that may result in harm to an asset
Risk	Probability of a threat exploiting a vulnerability
Vulnerability	A weakness that threatens the confidentiality, integrity, or availability (CIA) of an asset
CIA triad (confidentiality, integrity, availability)	The three main principles of IT security
Exploit	Using a tool or technique to take advantage of a vulnerability
Risk management	Process of identifying, assessing, and reducing risk to an acceptable level
Exposure	The estimated cost, loss, or damage that can result if a threat exploits a vulnerability
Access control	Security feature designed to restrict who has access to a network, IS, or data
Countermeasure	Safeguard implemented to mitigate (lessen) risk
Audit	The process of generating, recording, and reviewing a chronological record of system events to determine their accuracy
Encryption	Transformation of data into scrambled code to protect it from being understood by unauthorized users
Plaintext or clear-text	Readable text
Ciphertext	Encrypted text
Authentication	Method (usually based on username and password) by which an IS validates or verifies that a user is really who he or she claims to be
Malware (short for *malicious software)*	A generic term that refers to a virus, worm, Trojan horse, spyware, or adware
Scareware, also known as *rogueware* or *fake antivirus software*	Programs that pretend to scan a computer for viruses and then tell the user the computer is infected in order to convince the victim to voluntarily provide credit card information to pay $50 to $80 to "clean" the PC. When the victims pays the fee, the virus appears to vanish, but the machine is then infected by other malicious programs. It is one of the fastest-growing and most prevalent types of Internet fraud.
Biometrics	Methods to identify a person based on a biological feature, such as a fingerprint or retina
Perimeter security	Security measures to ensure that only authorized users gain access to the network
Endpoint security	Security measures to protect *endpoints*, e.g., desktops, laptops, and mobile devices
Firewall	Software or hardware device that controls access to a private network from a public network (Internet) by analyzing data packets entering or exiting it
Packet	A unit of data for transmission over a network with a *header* containing the source and destination of the packet
IP address (Internet Protocol address)	An address that uniquely identifies a specific computer or other device on a network
Public key infrastructure (PKI)	A system based on encryption to identify and authenticate the sender or receiver of an Internet message or transaction
Intrusion detection system (IDS)	A defense tool used to monitor network traffic (packets) and provide alerts when there is suspicious traffic or to quarantine suspicious traffic
Router	Device that transfers (routes) packets between two or more networks
Fault tolerance	The ability of an IS to continue to operate when a failure occurs, but usually for a limited time or at a reduced level
Backup	A duplicate copy of data or programs kept in a secured location
Spoofing	An attack carried out using a trick, disguise, deceit, or by falsifying data
Denial of service (DoS) or Distributed denial of service (DDoS)	An attack in which a system is bombarded with so many requests (for service or access) that it crashes or cannot respond
Zombie	An infected computer that is controlled remotely via the Internet by an unauthorized user, such as a spammer, fraudster, or hacker
Spyware	Stealth software that gathers information about a user or a user's online activity
Botnet (short for *Bot network*)	A network of hijacked computers that are controlled remotely—typically to launch spam or spyware. Also called software robots. Botnets are linked to a range of malicious activity, including identity theft and spam.

- In May 2006, the theft of a laptop during a home burglary of a Veterans Affairs employee cost taxpayers $100 million to remedy. See *IT at Work 5.1* for a description of the Department of Veterans Affairs data theft.
- In 2007, TJX Companies disclosed that data from 100 million credit and debit cards had been stolen by hackers starting in 2005. TJX's data heist was the largest breach ever to date, based on the number of records involved. Following the disclosure, banks said that tens of millions of dollars of fraudulent charges were made on the cards. The Massachusetts Bankers Association sued TJX for negligence. The FTC filed a complaint, alleging TJX did not have the proper security measures in place to prevent unauthorized access to the sensitive, personal customer information. The total cost of the data breach was an estimated $197 million.
- In November 2007, the United Kingdom's tax agency disclosed that it had lost unencrypted disks containing personal data, bank details, and national ID numbers on 25 million juvenile benefits claimants. Analyst firm Gartner Inc. estimated that closing compromised accounts and establishing new ones cost British banks about $500 million.

These incidents point out that victims of breaches are often third parties, such as customers, patients, social network users, credit card companies, and shareholders; costs to repair damage may be staggering.

Cloud Computing and Social Network Risks With the popularity of eReaders, netbooks, Google's Chrome OS, Facebook, YouTube, Twitter, LinkedIn, and other social networks, IT security dangers are getting worse. Social networks and cloud computing increase vulnerabilities by providing a single point of failure and attack for organized criminal networks. Critical, sensitive, and private information is at risk, and like previous IT trends, such as wireless networks, the goal is connectivity, often

IT at Work 5.1

$100 Million Data Breach at the U.S. Department of Veterans Affairs

One of the largest single thefts of personal data occurred on May 3, 2006, when a laptop and external hard drive belonging to the U.S. Department of Veterans Affairs (VA) were stolen during a home burglary. The VA reported that data on 26.5 million veterans and spouses was stored in plaintext (not encrypted) on the laptop stolen from the home of a senior-level IT specialist. He had taken the laptop and data from the office to do after-hours work. The data included veterans' names, birth dates, and Social Security numbers. VA Secretary Jim Nicholson testified before Congress that it would cost at least $10 million to inform veterans of the security breach.

VA Ignored Risks and Failed to Enforce Security Policy. The VA's policy required all personnel to encrypt sensitive data and prohibited them from removing VA data from their offices. Employees either had not been informed of the policy, however, or they realized it was not being enforced. In fact, the IT specialist, who had access to sensitive information, admitted he had been taking data home since 2003.

After the Security Breach. To mitigate the VA's risks, Nicholson promised:

- To have all VA employees take cybersecurity and privacy training courses
- To increase background checks of employees with access to sensitive information
- To review data access controls to minimize employees' access to sensitive data

Despite the enormous cost of the VA's data breach, it may not scare companies into more rigorous security policy monitoring and training. Rick LeVine, a senior manager in Accenture's global security practice (a consulting company; *accenture.com*), predicted that "It's going to take several high-profile incidents at Fortune 500 companies to cause people to say, 'Oh, my God, one guy's cell phone can lose us a billion dollars'" (Spangler, 2006).

Sources: Condensed from Spangler (2006) and several articles from the *Washington Post* and *InformationWeek*, May–June 2006.

Discussion Questions: Could such a massive security breach happen at any company? Why or why not? Do you agree with LeVine's prediction? What prediction would you make?

with little concern for security. As social networks increase their services, the gap between services and infosec also increases. E-mail viruses and malware have been declining for years as e-mail security has improved. This trend continues as communication shifts to social networks and newer smartphones. Unfortunately, malware finds its way to users through security vulnerabilities in these new services and devices. Web filtering, user education, and strict policies are key to preventing widespread outbreaks.

In Twitter and Facebook, users invite in others and build relationships with them. Cybercriminals hack into these trusted relationships using stolen log-ins. Fake antivirus and other attacks that take advantage of user trust are very difficult to detect.

An overriding reason why these networks and services increase exposure to risk is the **time-to-exploitation** of today's sophisticated spyware and mobile viruses. Time-to-exploitation is the elapsed time between when vulnerability is discovered and when it's exploited, or compromised by an attacker. That time has shrunk from months to minutes, so IT staff have ever-shorter timeframes to find and fix flaws before being compromised by an attack. Some attacks exist for as little as two hours, which means that enterprise IT security systems must have real-time protection. As of 2011, they will look to cloud services for enhanced security.

When new vulnerabilities are found in operating systems, applications, or wired and wireless networks, patches are released by the vendor or security organization. **Patches** are software programs that users download and install to fix the vulnerability. Microsoft, for example, releases patches that it calls **service packs** to update and fix vulnerabilities in its operating systems, including Vista, and applications, including Office 2007. Service packs are made available at Microsoft's Web site.

Left undetected or unprotected, vulnerabilities provide an open door for IT attacks, which lead to business disruptions and their financial damages. Despite even the best technology defenses, infosec incidents will occur mostly because of users who do not follow secure computing practices and procedures.

Phishing and Web-Based Threats Companies increasingly adopt external, Web-based applications and employees bring consumer applications into the enterprise. Criminal enterprises are following the money on the Internet, where they have a global market of potential victims.

(*Stuart Hickling/iStockphoto*)

Since 2007, Web-based threats have been the primary way of stealing confidential data and infecting computers. In 2008, two-thirds of all known malware was created. Then in the first half 2009, new malware exceeded all malware detected in 2008, phishing increased 585 percent, and more than 300 corporate brands were victimized. **Phishing** is a deceptive attempt to steal a person's confidential information by pretending to be a legitimate organization, such as PayPal, a bank, credit card company, or casino. Phishing messages include a link to a fraudulent phish Web site that looks like the real one. When the user clicks the link to the phish site, he or she is asked for a credit card number, Social Security number, account number, or password. In 2010 and 2011, phishing increased exponentially because unaware users still fall for the ruse.

Criminals use the Internet and private networks to hijack large numbers of PCs to spy on users, spam them, shake down businesses, and steal identities. But why are they so successful? The Information Security Forum (*securityforum.org*), a self-help organization that includes many Fortune 100 companies, compiled a list of the top information problems and discovered that nine of the top ten incidents were the result of three factors:

- Mistakes or human error
- Malfunctioning systems
- Misunderstanding the effects of adding incompatible software to an existing system

Unfortunately, these factors can often overcome the IT security technologies that companies and individuals use to protect their information. A fourth factor identified by the Security Forum is motivation, as described in *IT at Work 5.2.*

IT at Work 5.2

Money Laundering, Organized Crime, and Terrorist Financing

According to the U.S. Department of State (*state.gov*), transnational organized crime groups have long relied on money laundering to fund their operations. This practice poses international and national security threats. It undermines free enterprise by crowding out the private sector, and it threatens the financial stability of countries.

Funds used to finance terrorist operations are very difficult to track. Despite this obscurity, by adapting methods used to combat money laundering, such as financial analysis and investigations, authorities can significantly disrupt the financial networks of terrorists and build a paper trail and base of evidence to identify and locate leaders of terrorist organizations and cells.

International organized crime syndicates, al-Qaeda groups, and other cybercriminals steal hundreds of billions of dollars every year. Cybercrime is safer and easier than selling drugs, dealing in black market diamonds, or robbing banks. Online gambling offers easy fronts for international money-laundering operations.

Sources: Compiled from the U.S. Department of State (2008), Altman (2006), and Wolfe (2006).

Search Engine Manipulation Search engine manipulation is method used by cybercriminals to exploit search engine algorithms to position hacked Web sites higher in the ranking results. Such manipulation drives users to malicious sites, such as bait pages that offer fake antivirus or *warez* (pirated software, games, music, etc.). Malware spread through search engines is also increasing because of the high degree of trust users place in search engines and the ease with which rankings can be manipulated.

Multi-Link Attacks Attacks are getting more complex by being linked together. For example, search engine–manipulated links may connect to hacked blog pages that link to malware, which can download without the user's knowledge or consent. These linked attacks are designed to have a specific path; they do not work if the user does not follow that path. This *path-awareness* makes it very difficult for traditional Web crawlers to find and identify threats. Multi-link attacks will become part of more complex, blended threats as cybercriminals employ more layered approaches to avoid detection.

We now discuss government regulations and industry standards designed to force companies to invest in infosec defenses.

GOVERNMENT REGULATIONS

Data must be protected against existing and future attack schemes, and IT defenses must satisfy ever-stricter government and international regulations. Primary regulations are the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLB), Federal Information Security Management Act (FISMA), and USA Patriot Act in the United States; Japan's Personal Information Protection Act; Canada's Personal Information Protection and Electronic Document Act (PIPEDA); Australia's Federal Privacy Act; the United Kingdom's Data Protection Act; and Basel III (global financial services). All mandate the protection of personal data. The director of the Federal Trade Commission's (FTC) Bureau of Consumer Protection warned that the agency would bring enforcement action against small businesses lacking adequate policies and procedures to protect consumer data.

Two accepted models for IT governance are **enterprise risk management (ERM)** and **COBIT (Control Objectives for Information and Related Technology).** ERM is a risk-based approach to managing an enterprise that integrates internal control, the Sarbanes-Oxley Act mandates, and strategic planning. ERM is intended to be part of routine planning processes rather than a separate initiative. The ideal place to start is with buy-in and commitment from the board and senior leadership.

COBIT, which is described in *IT at Work 5.3,* is an internationally accepted IT governance and control framework for aligning IT with business objectives, delivering value, and managing associated risks. It provides a reference for management, users, and IS audit, control, and security practitioners.

IT at Work 5.3

COBIT and IT Governance Best Practices

ACC FIN HRM IS OM ETHICS

IT governance is the supervision, monitoring, and control of the organization's IT assets. The IT Governance Institute (*itgi.org*) publishes Control Objectives for Information and Related Technology (COBIT), which many companies use as their IT governance guide. COBIT can be downloaded from *isaca.org*. According to a 2008 PricewaterhouseCoopers survey, most IT executives are aware of best-practices frameworks like COBIT, but very few have enough IT staff to implement all of the best practices.

The Sarbanes-Oxley Act requires that companies provide proof that their financial applications and systems are controlled (secured) to verify that financial reports can be trusted. This requires that IT security managers work with business managers to do a risk assessment to identify which systems depend on technical controls rather than on business process controls. To meet COBIT, IT systems should be based on the following three principles:

- *Principle of economic use of resources:* This principle acknowledges that the cost of infosec needs to be balanced with its benefits. It's the basic cost-benefit principle that you're familiar with. For example, you wouldn't spend more to protect your auto, home, or other asset than they were worth. Because it's possible, for instance, for companies to set a very low value on the confidential data of customers and employers and therefore avoid basic infosec defenses, the next two principles try to make sure that doesn't happen.
- *Principle of legality:* This principle requires that companies invest in infosec to meet minimum legal requirements. This is a basic security principle, just like having hand railings on stairways, fire extinguishers, and alarm systems.
- *Accounting principles:* These principles require that the integrity, availability, and reliability of data and information systems be maintained.

INDUSTRY STANDARDS

Industry groups impose their own standards to protect their customers and their members' brand images and revenues. One example is the **Payment Card Industry Data Security Standard (PCI DSS),** created by Visa, MasterCard, American Express, and Discover.

PCI DSS is required for all members, merchants, or service providers that store, process, or transmit cardholder data. Section 6.6 of the PCI DSS went into full effect in June 2008. In short, this section of PCI DSS requires merchants and card payment providers to make certain their Web applications are secure. If done correctly, it could reduce the number of Web-related security breaches.

PCI DSS Section 6.6 mandates that retailers ensure that Web-facing applications are protected against known attacks by applying either of the following two methods:

1. Have all custom application code reviewed for vulnerabilities by an application security firm.
2. Install an application layer firewall in front of Web-facing applications. Each application will have its own firewall to protect against intrusions and malware.

The purpose of the PCI DSS is to improve customers' trust in e-commerce, especially when it comes to online payments, and to increase the Web security of online merchants. To motivate following these standards, the penalties for noncompliance are severe. The card brands can fine the retailer and increase transaction fees for each credit or debit card transaction. A finding of noncompliance can be the basis for lawsuits.

CompTIA Infosec Survey In its 2008 information security survey, the Computing Technology Industry Association (CompTIA, *comptia.org*), a nonprofit trade group, reported how companies in the United States, United Kingdom, Canada, and China are attempting to improve their infosec standards. Key findings are the following:

- Nearly 66 percent of U.S. firms, 50 percent of U.K. and Chinese firms, and 40 percent of Canadian firms have implemented written IT security policies.
- The percentage of IT budget that companies dedicate to security is growing year after year. In the United States, companies spent 12 percent of their 2007 IT budget for security purposes, up from 7 percent in 2005. The bulk of the budget was used to buy security-related technologies.
- About 33 percent of U.S. firms require that IT staff be certified in network and data security; in China, 78 percent of firms require IT security certification.

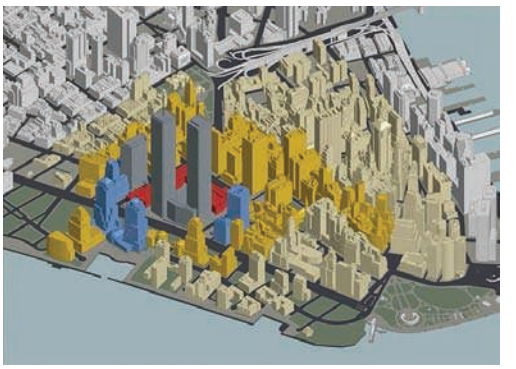

Figure 5.2 Lower Manhattan, the most communications-intensive real estate in the world.

IT security remains a major concern of IT professionals around the world according to *CompTIA's7th Annual Trends in Information Security: An Analysis of IT Security and the Workforce study.* As IT's role within an organization continues to expand, so does the potential for security breaches.

INFOSEC BREAKDOWNS BEYOND COMPANY CONTROL

Some types of incidents are beyond a company's control. The volcanic ash from Iceland in 2010 created prolonged disruptions and crises that had never been experienced by businesses. Uncertain events that can cause IS breakdowns, such as in the following incidents, require disaster recovery and business continuity plans, which are covered in Section 5.6.

Incident 1. Cybercriminals had launched an attack to extort money from StormPay, an online payment processing company. The attack shut down both of StormPay's data centers and its business for two days, causing financial loss and upsetting 3 million customers.

Incident 2. Lower Manhattan (see Figure 5.2) is the most communications-intensive real estate in the world. Many companies there lacked off-site-based business continuity plans and permanently lost critical data about their employees, customers, and operations in the aftermath of the September 11, 2001, attacks. Mission-critical systems and networks were brought down. They also lost network and phone connectivity when 7 World Trade Center (WTC) collapsed and Verizon's central office (CO)—which was located directly across from the WTC—suffered massive structural damage. In all, 300,000 telephone lines and 3.6 million high-capacity data circuits served by that CO were put out of service.

These incidents illustrate the diversity of infosec problems and the substantial damage that can be done to organizations anywhere in the world as a result.

IT SECURITY DEFENSE-IN-DEPTH MODEL

Defense-in-depth is a multilayered approach to infosec. The basic principle is that when one defense layer fails, another layer provides protection. For example, if a wireless network's security was compromised, then having encrypted data would still protect the data provided that the thieves could not decrypt it.

The success of any type of IT project depends on the commitment and involvement of executive management, also referred to as the "tone at the top." The same is true of IT security. When senior management shows its commitment to IT security, it becomes important to others, too. This infosec *tone* makes users aware that insecure practices and mistakes will not be tolerated. Therefore, an IT security and internal control model begins with senior management commitment and support, as shown in Figure 5.3. The model views infosec as a combination of people, processes, and technology.

Step 1: Senior management commitment and support. Senior managers' influence is needed to implement and maintain security, ethical standards, privacy practices, and internal control. The Committee of Sponsoring Organizations of the Treadway

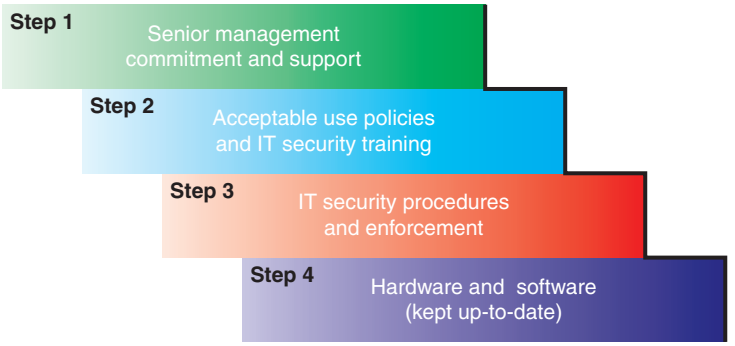

Figure 5.3 IT security defense-in-depth model.

Commission (COSO, *coso.org/key.htm*) defines **internal control** as a *process* designed to provide *reasonable* assurance of effective operations and reliable financial reporting. Internal control is discussed in Section 5.6.

Step 2: Acceptable use policies and IT security training. The next step in building an effective IT security program is to develop security policies and provide training to ensure that everyone is aware of and understands them. The greater the understanding of how security affects production levels, customer and supplier relationships, revenue streams, and management's liability, the more security will be incorporated into business projects and proposals.

Most critical is an **acceptable use policy (AUP)** that informs users of their responsibilities. An AUP is needed for two reasons: (1) to prevent misuse of information and computer resources and (2) to reduce exposure to fines, sanctions, and legal liability. To be effective, the AUP needs to define users' responsibilities, acceptable and unacceptable actions, and consequences of noncompliance. E-mail, Internet, and computer AUPs should be thought of as an extension of other corporate policies, such as those that address physical safety, equal opportunity, harassment, and discrimination.

Step 3: IT security procedures and enforcement. If users' activities are not monitored for compliance, the AUP is useless. Therefore, the next step is to implement monitoring procedures, training, and enforcement of the AUP. Businesses cannot afford the infinite cost of perfect security, so they calculate the proper level of protection. The calculation is based on the digital assets' risk exposure. The risk exposure model for digital assets is comprised of the five factors shown in Table 5.2.

Another risk assessment method is the **business impact analysis (BIA).** BIA is an exercise that determines the impact of losing the support or availability of a resource. For example, for most people, the loss of a smartphone would have greater impact than the loss of a digital camera. BIA helps identify the minimum resources needed to recover and prioritizes the recovery of processes and supporting systems. A BIA needs to be updated as new threats to IT emerge. After the risk exposure of

TABLE 5.2 Risk Exposure Model for Digital Assets

Factor	Cost and Operational Considerations
1. Asset's value to the company	What are the costs of replacement, recovery, or restoration? What is the recoverability time?
2. Attractiveness of the asset to a criminal	What is the asset's value (on a scale of low to high) to identity thieves, industrial spies, terrorists, or fraudsters?
3. Legal liability attached to the asset's loss or theft	What are the potential legal costs, fines, and restitution expenses?
4. Operational, marketing, and financial consequences	What are the costs of business disruption, delivery delays, lost customers, negative media attention, inability to process payments or payroll, or a drop in stock prices?
5. Likelihood of a successful attack against the asset	Given existing and emerging threats, what is the probability the asset will be stolen or compromised?

digital assets has been estimated, then informed decisions about investments in infosec can be made.

Step 4: Hardware and software. The last step in the model is implementation of software and hardware needed to support and enforce the AUP and secure practices.

Keep in mind that security is an ongoing and unending process, not a problem that can be solved with hardware or software. Hardware and software security defenses cannot protect against irresponsible business practices.

Review Questions

1. Why are cleanup costs after a single data breach or infosec incident in the tens of millions of dollars?
2. Who are the potential victims of an organization's data breach?
3. What is time-to-exploitation? What is the trend in the length of such a time?
4. What is a multi-link attack?
5. What is a service pack?
6. What are two causes of the top information problems at organizations?
7. What is an acceptable use policy (AUP)? Why do companies need an AUP?

5.2 IS Vulnerabilities and Threats

One of the biggest mistakes managers make is underestimating IT vulnerabilities and threats. Most workers use their laptops and mobiles for both work and leisure, and in an era of multitasking, they often do both at the same time. Yet off-time or off-site use of devices remains risky because, despite policies, employees continue to engage in dangerous online and communication habits. Those habits make them a weak link in an organization's otherwise solid security efforts. These threats can be classified as *unintentional or intentional.*

UNINTENTIONAL THREATS

Unintentional threats fall into three major categories: human errors, environmental hazards, and computer system failures.

- **Human errors** can occur in the design of the hardware or information system. They can also occur during programming, testing, or data entry. Not changing default passwords on a firewall or failing to manage patches create security holes. Human errors also include untrained or unaware users responding to phishing or ignoring security procedures. Human errors contribute to the majority of internal control and infosec problems.
- **Environmental hazards** include volcanoes, earthquakes, blizzards, floods, power failures or strong fluctuations, fires (the most common hazard), defective air conditioning, explosions, radioactive fallout, and water-cooling-system failures. In addition to the primary damage, computer resources can be damaged by side effects, such as smoke and water. Such hazards may disrupt normal computer operations and result in long waiting periods and exorbitant costs while computer programs and data files are re-created.
- **Computer systems failures** can occur as the result of poor manufacturing, defective materials, and outdated or poorly maintained networks (recall the network crash at LAX airport discussed in Chapter 4). Unintentional malfunctions can also happen for other reasons, ranging from lack of experience to inadequate testing.

INTENTIONAL THREATS

Examples of intentional threats include theft of data; inappropriate use of data (e.g., manipulating inputs); theft of mainframe computer time; theft of equipment and/or programs; deliberate manipulation in handling, entering, processing, transferring, or programming data; labor strikes, riots, or sabotage; malicious damage to computer resources; destruction from viruses and similar attacks; and miscellaneous computer abuses and Internet fraud. The scope (target) of intentional threats can be against an entire country or economy.

Hackers tend to involve unsuspecting insiders in their crimes, using tactics called **social engineering.** From an infosec perspective, social engineering has been used by criminals or corporate spies to trick insiders into revealing information or access codes that outsiders should not have. A common tactic used by hackers to get access to a network is to call employees pretending to be the network administrator who wants to solve a serious problem. To solve the problem, they need the employee to give them their password. Of course, the tactic won't work on employees who have been trained not to give out passwords over the phone to anyone.

Malware creators have also used social engineering to maximize the range or impact of their viruses, worms, and so on. For example, the *ILoveYou* worm used social engineering to entice people to open malware-infected e-mail messages. The *ILoveYou* worm attacked tens of millions of Windows computers in May 2000 when it was sent as an e-mail attachment with the subject line: ILOVEYOU. Often out of curiosity, people opened the attachment named LOVE-LETTER-FOR-YOU.TXT.vbs—releasing the worm. Within nine days, the worm had spread worldwide, crippling networks, destroying files, and causing an estimated $5.5 billion in damages. Notorious hacker Kevin Mitnick, who served time in jail for hacking, used social engineering as his primary method to gain access to computer networks. In most cases, the criminal never comes face-to-face with the victim but communicates via the phone or e-mail.

Not all hackers are malicious, however. *White-hat hackers* perform ethical hacking, such as performing penetrating tests on their clients' systems or searching the Internet to find the weak points so they can be fixed. White-hat hacking by Finjan, an information security vendor, for example, led to the discovery of a **crime server** in Malaysia in April 2008, as described in *IT at Work 5.4*. A crime server is a server used to store stolen data for use in committing crimes. Finjan discovered the crime server while running its real-time code inspection technology to diagnose customers' Web traffic.

Social engineering is used for (noncriminal) business purposes, too. For example, commercials use social engineering (e.g., promises of wealth or happiness) to convince people to buy their products or services.

IT ATTACKS

There are many types of attack, and new ones appear regularly. Two basic types of deliberate attacks are data tampering and programming attack.

Data tampering is a common means of attack that is overshadowed by other types of attacks. It refers to an attack during which someone enters false or fraudulent data into a computer or changes or deletes existing data. Data tampering is extremely serious because it may not be detected. This is the method often used by insiders and fraudsters.

IT at Work 5.4

1.4 Gigabytes of Stolen Data and E-Mail Found on Crime Server

In April 2008, Finjan software researchers found compromised data from patients, bank customers, business e-mail messages, and Outlook accounts on a Malaysia-based server. Data included usernames, passwords, account numbers, Social Security and credit card numbers, patient data, business-related e-mail communications, and captured Outlook accounts containing e-mails. The stolen data, all less than one month old, consisted of 5,388 unique log files from around the world. The server had been running for three weeks before it was found. Data had been stolen from victims in the United States, Germany, France, India, England, Spain, Canada, Italy, the Netherlands, and Turkey. More than 5,000 customer records from 40 international financial institutions had been stolen.

A crime server held more than 1.4 gigabytes of business and personal data stolen from computers infected with Trojan horses. While gathering data, it also acted as a command-and-control server for the malware (also called crimeware) that ran on the infected PCs. The command-and-control applications enabled the hacker to manage the actions and performance of the crimeware, giving the hacker control over the uses of the crimeware and its victims. Since the crime server's stolen data was left without any access restrictions or encryption, the data was freely available to anyone on the Web. This was not an isolated situation. Two other crime servers holding similar information were found and turned over to law enforcement for investigation.

Sources: Compiled from Higgins (2008) and McGlasson (2008).

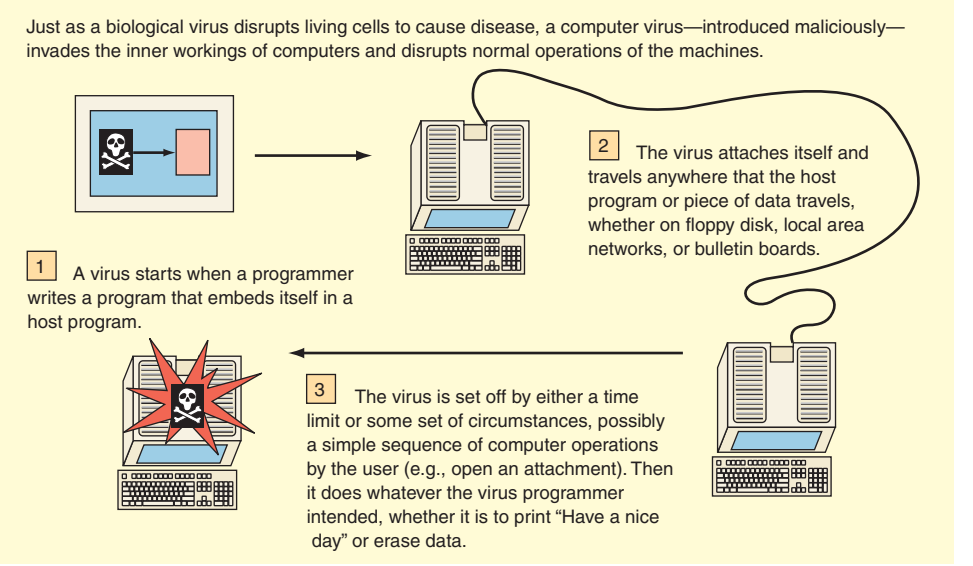

Figure 5.4 How a computer virus can spread.

Programming attacks are popular with criminals who use programming techniques to modify other computer programs. For these types of crimes, programming skill and knowledge of the targeted systems are needed. Malware examples are viruses, worms, and Trojan horses. Several of the methods were designed for Web-based systems. Malware can be used to launch **denial of service (DoS) attacks.** A DoS attack occurs when a server or Web site receives a flood of traffic—much more traffic or requests for service than it can handle, causing it to crash.

A universal attack method is the **virus,** which is computer code (software program). It receives its name from the program's ability to attach itself to and infect other computer programs, without the owner of the program being aware of the infection, as shown in Figure 5.4. When the infected software is used, the virus spreads, causing damage to that program and possibly to others.

Unlike a virus, a **worm** spreads without any human intervention, such as checking e-mail or transmitting files. Worms use networks to propagate and infect anything attached to them—including computers, handheld devices, Web sites, and servers. Worms can spread via instant or text messages. Worms' ability to self-propagate through a network can clog and degrade a network's performance, including the Internet.

Trojan horses are referred to as backdoors because they give the attacker illegal access to a network or account through a network port. A network port is a physical interface for communication between a computer and other devices on a network. **Remote administration Trojans (RATs)** are a class of backdoors that enable remote control over the compromised (infected) machine. The crime server discussed in *IT at Work 5.4* involved RAT-infected computers for stealth data collection. RATs open a network port on a victim computer, giving the attacker control over it. Infected PCs are also called *zombies* or *bots*.

A Trojan attaches itself to a zombie's OS and always has two files, the client file and the server file. The server, as its name implies, is installed in the infected machine while the client is used by the intruder to control the compromised system. Trojan horse functions include managing files on the zombie PC, managing processes, remotely activating commands, intercepting keystrokes, watching screen images, and restarting and closing down infected hosts. Common trojans are NetBus, Back Orifice (BO) 2000, SubSeven, and Hack'a'tack.

TARGETED ATTACKS ON ENTERPRISES

Corporate and government secrets are currently being stolen by a serious threat called **advanced persistent threat (APT).** Most APT attacks are launched through phishing. Typically, this type of attack begins with some reconnaissance on the part of attackers. This can include researching publicly available information about the

company and its employees, often from social networking sites. This information is then used to create targeted phishing e-mail messages. A successful attack could give the attacker access to the enterprise's network.

APTs are designed for long-term espionage. Once installed on a network, APTs transmit copies of documents, such as Microsoft Office files and PDFs, in stealth mode. APTs collect and store files on the company's network, encrypt them, then sends them in bursts to servers, typically in China.

A notorious APT is *Hydraq Trojan*, or *Aurora.* In January 2010, dozens of large companies were compromised by *Hydraq*. In the Hydraq attack, a previously unknown vulnerability in Microsoft Internet Explorer and a patched vulnerability in Adobe Reader and Flash Player are exploited to install the Trojan. Once installed, attackers may have full remote access to do whatever they want. Typically, once they have established access within the enterprise, attackers use their access privileges to connect to other computers and servers and compromise them, too. They can do this by stealing credentials on the local computer or capturing data by installing a keystroke logger.

APT attacks are designed to remain undetected in order to gather information over prolonged periods. This type of attack has been observed in other large-scale data breaches that exposed large numbers of identities.

BOTNETS

A **botnet** is a collection of bots (computers infected by software robots). Those infected computers, called **zombies,** can be controlled and organized into a network of zombies on the command of a remote botmaster (also called *bot herder*). Storm worm, which is spread via spam, is a botnet agent embedded inside over 25 million computers. Storm's combined power has been compared to the processing might of a supercomputer, and Storm-organized attacks are capable of crippling any Web site.

Botnets expose infected computers, as well as other network computers, to the following threats (Edwards, 2008):

- **Spyware:** Zombies can be commanded to monitor and steal personal or financial data.
- **Adware:** Zombies can be ordered to download and display advertisements. Some zombies even force an infected system's browser to visit a specific Web site.
- **Spam:** Most junk e-mail is sent by zombies. Owners of infected computers are usually blissfully unaware that their machines are being used to commit a crime.
- **Phishing:** Zombies can seek out weak servers that are suitable for hosting a phishing Web site, which looks like a legitimate Web site, to trick the users into inputting confidential data.
- **DoS Attacks:** In a *denial of service* attack, the network or Web site is bombarded with so many requests for service (that is, traffic) that it crashes.

Botnets are extremely dangerous because they scan for and compromise other computers and then can be used for every type of crime and attack against computers, servers, and networks.

MALWARE AND BOTNET DEFENSES

Since malware and botnets use many attack methods and strategies, multiple tools are needed to detect them and/or neutralize their effects. Three essential defenses are the following:

1. **Antivirus software:** Anti-malware tools are designed to detect malicious codes and prevent users from downloading them. They can also scan systems for the presence of worms, Trojan horses, and other types of threats. This technology does not provide complete protection because it cannot defend against *zero-day exploits*. *Zero-day* refers to the day the exploits hit the Internet. Anti-malware may not be able to detect a previously unknown exploit.
2. **Intrusion detection systems (IDS):** As the name implies, an IDS scans for unusual or suspicious traffic. An IDS can identify the start of a DoS attack by the traffic pattern, alerting the network administrator to take defensive action, such as switching to another IP address and diverting critical servers from the path of the attack.

3. Intrusion prevention systems (IPS): An IPS is designed to take immediate action—such as blocking specific IP addresses—whenever a traffic-flow anomaly is detected. ASIC (application-specific integrated circuit)-based IPSs have the power and analysis capabilities to detect and block DoS attacks, functioning somewhat like an automated circuit breaker.

Lavasoft (*lavasoft.com/*) offers free software, called Ad-Aware, to identify and remove Trojans and other infections at *lavasoft.com*. Its Web site also provides news about current malware threats.

In the next section, we discuss crime, one example of which is fraud, or white-collar crime. Companies suffer tremendous loss from occupational fraud. It is a widespread problem that affects every company, regardless of size, location, or industry. The FBI has labeled fraud one of the fastest-growing crimes.

Review Questions

1. Define and give three examples of an unintentional threat.
2. Define and give three examples of an intentional threat.
3. What is social engineering? Give an example.
4. What is a crime server?
5. What are the risks from data tampering?
6. List and define three types of malware.
7. Define *botnet* and explain its risk.
8. Explain the difference between an IDS and an IPS.

5.3 Fraud, Crimes, and Violations

Crime can be divided into two categories depending on the tactics used to carry it out: violent and nonviolent. Fraud is nonviolent crime because instead of a gun or knife, fraudsters use deception and trickery. Fraudsters carry out their crime by abusing the power of their position or by taking advantage of the trust, ignorance, or laziness of others.

FRAUD

Occupational fraud refers to the deliberate misuse of the assets of one's employer for personal gain. Internal audits and internal controls are essential to the prevention and detection of occupation frauds. Several examples are listed in Table 5.3.

High-profile cases of occupational fraud committed by senior executives, such as Bernard Madoff, have led to increased government regulation. However, increased legislation has not put an end to fraud. *IT at Work 5.5* gives some insight into Madoff's $50 billion fraud, which also led to the investigation of the agency responsible for fraud prevention—the SEC (Securities and Exchange Commission, *sec.gov/*).

TABLE 5.3 Types and Characteristics of Organizational Fraud

Type of Fraud	Does This Fraud Impact Financial Statements?	Typical Characteristics
Operating management corruption	No	Occurs *off the books.* Median loss due to corruption: over six times greater than median loss due to misappropriation ($530,000 vs. $80,000)
Conflict of interest	No	A breach of confidentiality, such as revealing competitors' bids; often occurs with bribery
Bribery	No	Uses positional power or money to influence others
Embezzlement or "misappropriation"	No	Employee theft—employees' access to company property creates the opportunity for embezzlement
Senior management financial reporting fraud	Yes	Involves a massive breach of trust and leveraging of positional power
Accounting cycle fraud	Yes	This fraud is called "earnings management" or earning engineering, which are in violation of GAAP (generally accepted accounting principles) and all other accounting practices. See *aicpa.org*

IT at Work 5.5

Madoff Defrauds Investors of $64.8 Billion

Disgraced financier Bernard Madoff is in jail after pleading guilty in 2009 to the biggest fraud in Wall Street history.

For four decades, Madoff perpetrated a complex and sinister fraud. Prior to his arrest on December 11, 2008, Madoff was viewed as a charismatic man and stellar financier with favorable connections to power brokers on Wall Street and in Washington. Since his arrest, federal prosecutors have said that Bernard Madoff ran a scheme that bilked wealthy individuals and large nonprofits out of an estimated $64.8 billion.

Social Engineering. Fundamentally, Madoff relied on social engineering and the predictability of human nature to generate income for himself, not on financial expertise. Madoff would ask people to invest in his funds, which were by invitation only, to create the illusion of exclusivity. Madoff used this tactic to create the illusion that only the elite could invest because of consistent returns and his stellar Wall Street reputation. As he expected, wealthy investors mistook *exclusivity* to mean a secret formula for a *sure thing*.

Steady returns, an actual example of which is shown in Figure 5.5, were one of the many well-known red flags indicating fraud that investors and watchdogs chose to disregard. In fact, looking back, investors are saying they missed several glaring red flags.

Red Flags of Fraud. The classic red flags that made this fraud detectable much earlier (if those flags had not been ignored by many) include:

- Madoff was trusted because he was a Wall St. fixture, so his work was not given full scrutiny.
- The unbelievable returns defied the market. The returns were impossible, yet this fact was ignored.
- Madoff used a sense of exclusivity—a hook to play "hard to get." This false sense of exclusivity is a sign of a Ponzi scheme.
- There were steady returns. Reports of consistently good but never spectacular gains can lull all kinds of investors into a false sense of security over time.

Madoff and SEC Being Investigated. This scandal triggered investigations not only of Madoff but also of the watchdog agency, the Securities and Exchange Commission (SEC). The SEC was investigated by Congress and the agency's Inspector General for repeatedly ignoring whistleblowers' warnings about Madoff's operations. Created by Congress in 1934 during the Great Depression, the SEC is charged with ensuring that public companies accurately disclose their financial and business risks to investors and that brokers who trade securities for clients keep investors' interests first.

Madoff is not the only one at fault. He worked with dozens of feeder funds and other middlemen to lure money into his Ponzi scheme. Investigations have involved forensic accounting as well as computer forensics—the latter to discover a smoking-gun e-mail on other digital messages that reveal *who knew what* and *who did what*. Forensics experts are digging deep into the evidence to determine who else was complicit in the fraud.

Regulatory Reaction. In January 2009, the Senate Banking Committee introduced legislation to provide $110 million to hire 500 new FBI agents, 50 new assistant U.S. attorneys, and 100 new SEC enforcement officials to crack down on fraud.

Sources: Compiled from Antilla (2008), Appelbaum and Hilzenrath (2008), Chew (2009), Gold (2008), and Quinn (2009).

Discussion Questions: How important was trust to Madoff's scheme? What else did Madoff rely on to carry out his fraud? What is a *red flag*? In your opinion, how were so many red flags ignored given the risk that investors faced? Could a large investment fraud happen again—or are there internal fraud prevention and detection measures that would prevent it from happening? Explain your answer.

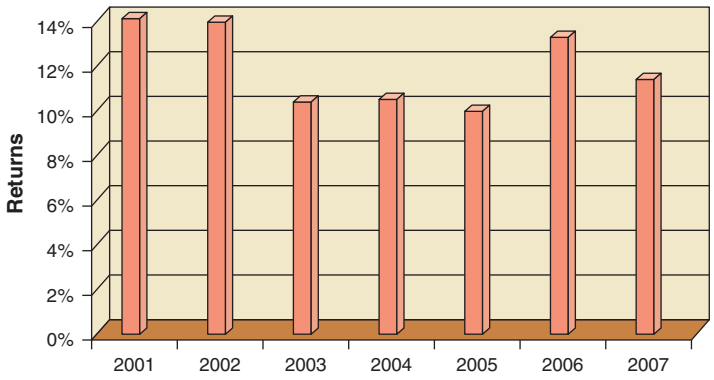

Figure 5.5 Annual Returns on a Madoff-Investor's Account from 2001–2007.

INTERNAL FRAUD PREVENTION AND DETECTION

IT has a key role to play in demonstrating effective corporate governance and fraud prevention. Regulators look favorably on companies that can demonstrate good corporate governance and best-practice operational risk management. Management and staff of such companies can then spend less time worrying about regulations and more time adding value to their brand and business.

Internal fraud prevention measures are based on the same controls used to prevent external intrusions—perimeter defense technologies, such as firewalls, e-mail scanners, and biometric access. They are also based on human resource (HR) procedures, such as recruitment screening and training.

ETHICS

Much of this detection activity can be handled by intelligent analysis engines using advanced data warehousing and analytics techniques. These systems take in audit trails from key systems and personnel records from the HR and finance departments. The data is stored in a data warehouse, where it is analyzed to detect anomalous patterns, such as excessive hours worked, deviations in patterns of behavior, copying of huge amounts of data, attempts to override controls, unusual transactions, and inadequate documentation about a transaction. Information from investigations is fed back into the detection system so that it learns. Since insiders might work in collusion with organized criminals, insider profiling is important to find wider patterns of criminal networks.

An enterprisewide approach that combines risk, security, compliance, and IT specialists greatly increases the prevention and detection of fraud. Prevention is the most cost-effective approach, since detection and prosecution costs are enormous, above and beyond the direct cost of the loss. Prevention starts with corporate governance culture and ethics at the top levels of the organization.

Identity Theft One of the worst and most prevalent crimes is identity theft. Such thefts, where individuals' Social Security and credit card numbers are stolen and used by thieves, are not new. Criminals have always obtained information about other people—by stealing wallets or digging in dumpsters. But widespread electronic sharing and databases have made the crime worse. Because financial institutions, data processing firms, and retail businesses are reluctant to reveal incidents in which their customers' personal financial information may have been stolen, lost, or compromised, laws continue to be passed to force those notifications. Examples in Table 5.4 illustrate different ways in which identity theft crimes have occurred.

TABLE 5.4 Examples of Identity Crimes Requiring Notification

How It Happened	Number of Individuals Notified	Description
Stolen desktop	3,623	Desktop computer was stolen from regional sales office containing data that was password-protected but not encrypted. Thieves stole SSNs and other information from TransUnion LLC, which maintains personal credit histories.
Online, by an ex-employee	465,000	Former employee downloaded information about participants in Georgia State Health Benefits Plan.
Computer tapes lost in transit	3.9 million	CitiFinancial, the consumer finance division of Citigroup Inc., lost tapes containing information about both active and closed accounts while they were being shipped to a credit bureau.
Online "malicious user" used legitimate user's log-in information	33,000	The U.S. Air Force suffered a security breach in the online system containing information on officers and enlisted personnel, including personal information.
Missing backup	200,000	A timeshare unit of Marriott International lost a backup tape containing SSNs and other confidential data of employees and timeshare owners and customers.

Review Questions

1. What are the two types of crimes?
2. Define *fraud* and *occupational fraud*. Identify two examples of each.
3. How can internal fraud be prevented? How can it be detected?
4. Explain why data on laptops and computers should be encrypted.
5. Explain how identity theft can occur.

5.4 Information Assurance and Risk Management

The objective of IT security management practices is to defend all of the components of an information system, specifically data, software applications, hardware, and networks. Before they make any decisions concerning defenses, people responsible for security must understand the requirements and operations of the business, which form the basis for a customized defense strategy. In the next section, we describe the major defense strategies.

DEFENSE STRATEGY

The defense strategy and controls that should be used depend on what needs to be protected and the cost-benefit analysis. That is, companies should neither underinvest nor overinvest. The SEC and FTC impose huge fines for data breaches to deter companies from underinvesting in data protection. The following are the major objectives of defense strategies:

1. **Prevention and deterrence.** Properly designed controls may prevent errors from occurring, deter criminals from attacking the system, and, better yet, deny access to unauthorized people. These are the most desirable controls.
2. **Detection.** As with a fire, the earlier an attack is detected, the easier it is to combat and the less damage is done. Detection can be performed in many cases by using special diagnostic software, at a minimal cost.
3. **Containment (contain the damage).** Containment minimizes or limits losses once a malfunction has occurred. It is also called damage control. This can be accomplished, for example, by including a *fault-tolerant system* that permits operation in a degraded mode until full recovery is made. If a fault-tolerant system does not exist, a quick and possibly expensive recovery must take place. Users want their systems back in operation as fast as possible.
4. **Recovery.** A recovery plan explains how to fix a damaged information system as quickly as possible. Replacing rather than repairing components is one route to fast recovery.
5. **Correction.** Correcting the causes of damaged systems can prevent the problem from occurring again.
6. **Awareness and compliance.** All organization members must be educated about the hazards and must comply with the security rules and regulations.

A defense strategy also requires several controls, as shown in Figure 5.6. **General controls** are established to protect the system regardless of the specific application. For example, protecting hardware and controlling access to the data center are independent of the specific application. **Application controls** are safeguards that are intended to protect specific applications. In the next two sections, we discuss the major types of these two groups of information systems controls.

GENERAL CONTROLS

The major categories of general controls are physical controls, access controls, biometric controls, administrative controls, application controls, and endpoint controls.

Physical Controls Physical security refers to the protection of computer facilities and resources. This includes protecting physical property such as computers, data centers, software, manuals, and networks. It provides protection against most natural hazards

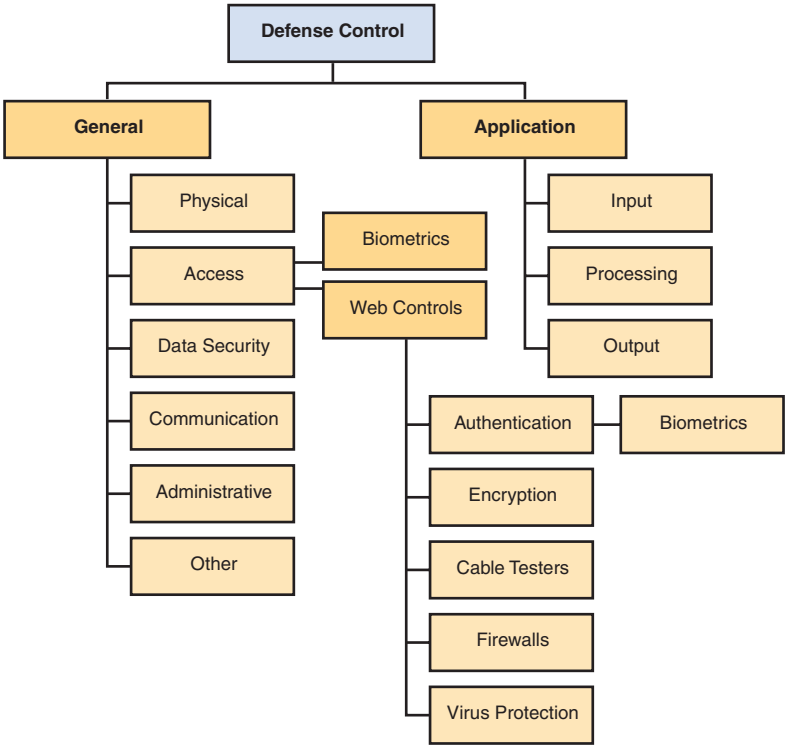

Figure 5.6 Major defense controls.

as well as against some human hazards. Appropriate physical security may include several controls, such as the following:

- Appropriate design of the data center; for example, ensuring that the data center is noncombustible and waterproof
- Shielding against electromagnetic fields
- Good fire prevention, detection, and extinguishing systems, including sprinkler system, water pumps, and adequate drainage facilities
- Emergency power shutoff and backup batteries, which must be maintained in operational condition
- Properly designed, maintained, and operated air-conditioning systems
- Motion detector alarms that detect physical intrusion

Access Controls Access control is the management of who is and is not authorized to use a company's hardware and software. Access control methods, such as firewalls and access control lists, restrict access to a network, database, file, or data. It is the major defense line against unauthorized insiders as well as outsiders. Access control involves authorization (having the right to access) and authentication, which is also called user identification (proving that the user is who he or she claims to be).

Authentication methods include:

- Something only the user knows, such as a password
- Something only the user has, such as a smart card or a token
- Something that is characteristic only of the user, such as a signature, voice, fingerprint, or retinal (eye) scan; implemented via biometric controls, which can be physical or behavioral

Biometric Controls A **biometric control** is an automated method of verifying the identity of a person, based on physical or behavioral characteristics. Most biometric

systems match some personal characteristic against a stored profile. The most common biometrics are the following:

- **Thumbprint or fingerprint.** Each time a user wants access, a thumb- or fingerprint (finger scan) is matched against a template containing the authorized person's fingerprint to identify him or her.
- **Retinal scan.** A match is attempted between the pattern of the blood vessels in the retina that is being scanned and a prestored picture of the retina.
- **Voice scan.** A match is attempted between the user's voice and the voice pattern stored on templates.
- **Signature.** Signatures are matched against the prestored authentic signature. This method can supplement a photo card ID system.

Biometric controls are now integrated into many e-business hardware and software products. Biometric controls do have some limitations: They are not accurate in certain cases, and some people see them as an invasion of privacy.

Administrative Controls While the previously discussed general controls are technical in nature, administrative controls deal with issuing guidelines and monitoring compliance with the guidelines. Examples of such controls are shown in Table 5.5.

Application Controls Sophisticated attacks are aimed at the application level, and many applications were not designed to withstand such attacks. For better survivability, information-processing methodologies are being replaced with agent technology. **Intelligent agents,** also called softbots or knowbots, are highly adaptive applications. The term generally means applications that have some degree of reactivity, autonomy, and adaptability—as is needed in unpredictable attack situations. An agent is able to adapt itself based on changes occurring in its environment, as shown in Figure 5.7.

In the next section, the focus is on the company's digital endpoints and the perimeter—the network. We discuss the security of wireline and wireless networks and their inherent vulnerabilities.

Endpoint Security and Control Many managers underestimate the business risk posed by unencrypted portable storage devices, which are examples of *endpoints*. Business data is often carried on thumb drives, smartphones, and removable memory cards without IT's permission, oversight, or sufficient protection against loss or theft. Handhelds and portable storage devices put sensitive data at risk. According to market research firm Applied Research-West, three of four workers save corporate data on thumb drives. According to their study, 25 percent save customer records, 17 percent store financial data, and 15 percent store business plans on thumb drives, but less than 50 percent of businesses routinely encrypt those drives and even less consistently secure data copied onto smartphones.

TABLE 5.5 Representative Administrative Controls

- Appropriately selecting, training, and supervising employees, especially in accounting and information systems
- Fostering company loyalty
- Immediately revoking access privileges of dismissed, resigned, or transferred employees
- Requiring periodic modification of access controls (such as passwords)
- Developing programming and documentation standards (to make auditing easier and to use the standards as guides for employees)
- Insisting on security bonds or malfeasance insurance for key employees
- Instituting separation of duties, namely, dividing sensitive computer duties among as many employees as economically feasible in order to decrease the chance of intentional or unintentional damage
- Holding periodic random audits of the system

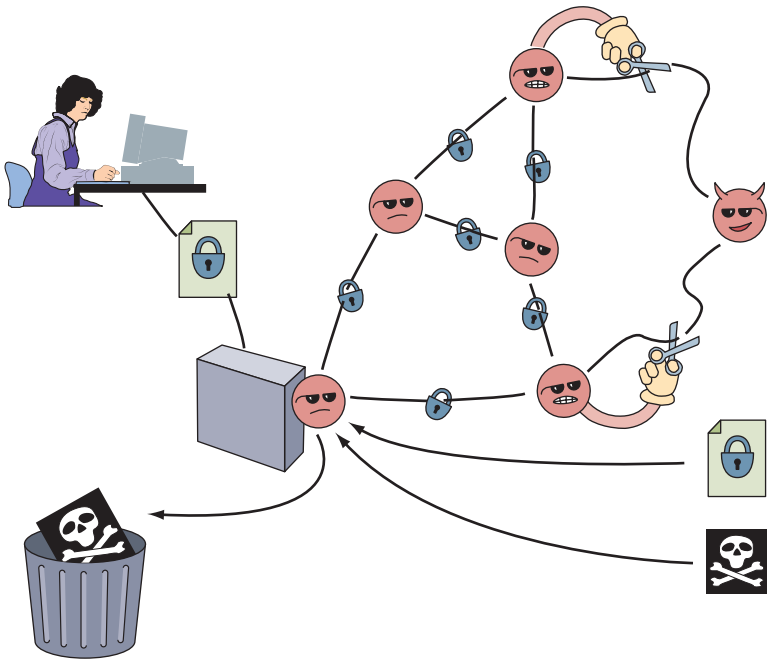

Figure 5.7 Intelligent agents. Agents in the collective communicate over secured links on the Internet or an intranet. Malicious agents (with horns) are detected and cut off from the collective. Properly authenticated data is allowed into the collective, but bad information is rejected. *Source: Courtesy of Sandia National Laboratories.*

Portable devices that store confidential customer or financial data must be protected no matter who owns it—employees or the company. If there are no security measures to protect handhelds or other mobile/portable storage, data must not be stored on them because it exposes the company to liability, lawsuits, and fines. For smaller companies, a single data breach could bankrupt the company.

Strong protection now requires more than native encryption. For example, locking a BlackBerry does not provide strong protection. Security company IronKey reported that Mantech Crowbar (*cybersolutions.mantech.com/*) can copy the contents of a BlackBerry's SD card quickly and crack a 4-digit PIN in 30 seconds. Crowbar, which costs about $2,300, is designed to be simple and fast at doing its one job—cracking passwords on MMC/SD cards. The Crowbar can crack security on a handheld device without alerting the owner that the device's security has been compromised. The Crowbar also stores log-in information for the cracked handheld, allowing a hacker to access the hacked device again unless the user changes the password.

Review Questions

1. What are the major objectives of a defense strategy?
2. What are general controls? What are application controls?
3. Define *access control*.
4. What are biometric controls? Give two examples.
5. What is the general meaning of *intelligent agents*?
6. What is endpoint security?
7. How does Mantech Crowbar increase endpoint risk?

5.5 Network Security

As a defense, companies need to implement network access control (NAC) products. NAC tools are different from traditional security technologies and practices that focus on file access. While file-level security is useful for protecting data, it does not keep unauthorized users out of the network in the first place. NAC technology, on the other hand, helps businesses lock down their networks against criminals.

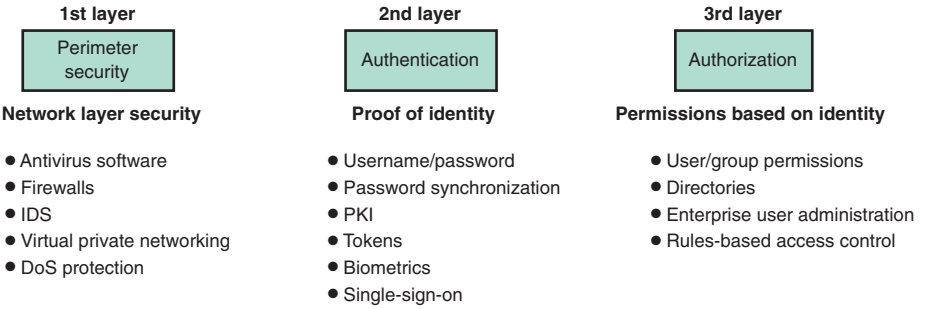

Figure 5.8 Three layers of network security measures.

Network security measures involve three types of defenses, which are referred to as *layers:*

- **First layer: Perimeter security** to control access to the network. Examples are antivirus software and firewalls.
- **Second layer: Authentication** to verify the identity of the person requesting access to the network. Examples are usernames and passwords.
- **Third layer: Authorization** to control what authenticated users can do once they are given access to the network. Examples are permissions and directories.

Details of these three defense layers are shown in Figure 5.8.

PERIMETER SECURITY AND FIREWALLS

The major objective of perimeter security is access control. The technologies used to protect against malware (e.g., firewalls, IDS, and IDP) also protect the perimeter. A firewall is a system, or group of systems, that enforces an access-control policy between two networks. It is commonly used as a barrier between a secure corporate intranet or other internal networks and the Internet, which is unsecured. Firewalls function by deciding what traffic to permit (allow) into and out of the network and what traffic to block. Firewalls need to be configured to enforce the company's security procedures and policies. A network has several firewalls, but they still cannot stop all malware (see Figure 5.9). For example, each virus has a signature, which identifies it. Firewalls and antivirus software that have been updated—and know of that virus's signature—can block it. But viruses pass through a firewall if the firewall cannot identify it as a virus. For example, a newly released virus whose signature has not yet been identified or that is hidden in an e-mail attachment can be allowed into the network. That's the reason why firewalls and antivirus software require continuous updating.

All Internet traffic, which travels as packets, should have to pass through a firewall, but that is rarely the case for instant messages and wireless traffic, which, as a result, "carry" malware into the network and applications on host computers. Firewalls do not control anything that happens after a legitimate user (who may be a disgruntled employee or an employee whose username and password have been compromised) has been authenticated and granted authority to access applications on the network. For these reasons, firewalls are a necessary but insufficient defense.

NETWORK AUTHENTICATION AND AUTHORIZATION

As applied to the Internet, an authentication system guards against unauthorized access attempts. The major objective of authentication is the proof of identity. The attempt here is to identify the legitimate user and determine the action he or she is allowed to perform.

Because phishing and identity theft prey on weak authentication, and usernames and passwords do not offer strong authentication, other methods are needed. There are **two-factor authentication** (also called multifactor authentication) and two-tier authentication. With two-factor authentication, other information is used to verify the user's identity, such as biometrics.

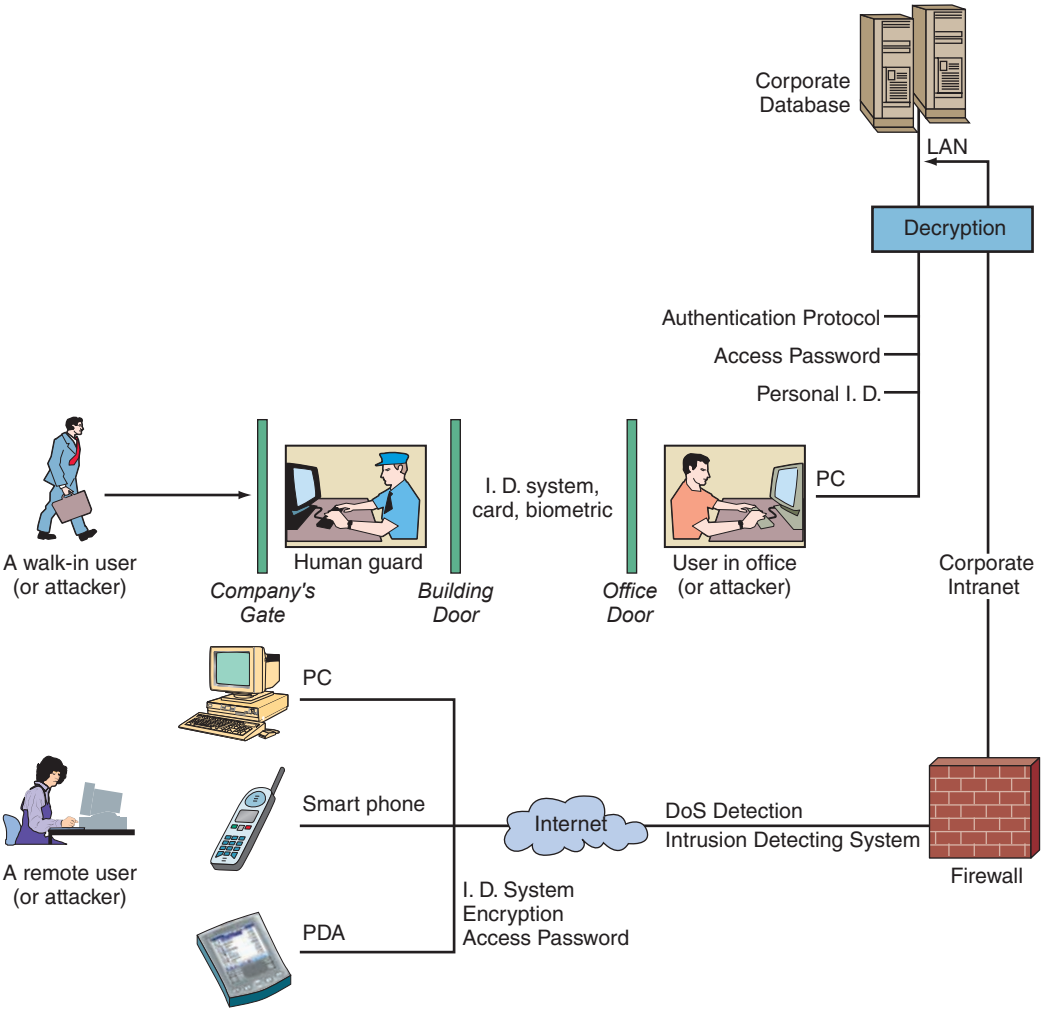

Figure 5.9 Where IT security mechanisms are located.

There are three key questions to ask when setting up an authentication system:

1. **Who are you?** Is this person an employee, a partner, or a customer? Different levels of authentication would be set up for different types of people.
2. **Where are you?** For example, an employee who has already used a badge to access the building is less of a risk than an employee or partner logging on remotely. Someone logging on from a known IP address is less of a risk than someone logging on from Nigeria or Kazakhstan.
3. **What do you want?** Is this person accessing sensitive or proprietary information or simply gaining access to benign data?

When dealing with consumer-facing applications, such as online banking and e-commerce, strong authentication must be balanced with convenience. If authentication makes it too difficult to bank or shop online, users will go back to the brick-and-mortars. There is a trade-off between increased protection and turning customers away from your online channel. In addition, authentication of a Web site to the customer is equally critical. E-commerce customers need to be able to identify whether it is a fraudulent site set up by phishers.

Authorization refers to permission issued to individuals or groups to do certain activities with a computer, usually based on verified identity. The security system, once it authenticates the user, must make sure that the user operates within his or her authorized activities.

SECURING WIRELESS NETWORKS

Wireless networks are more difficult to protect than wireline ones. All of the vulnerabilities that exist in a conventional wireline network apply to wireless technologies. Wireless access points (wireless APs or WAPs) behind a firewall and other security protections can be a backdoor into a network. Sensitive data that is not encrypted or is encrypted with a weak cryptographic technique used for wireless, such as **wired equivalent privacy (WEP),** and that is transmitted between two wireless devices, may be intercepted and disclosed. Wireless devices are susceptible to DoS attacks because intruders can gain access to network management controls and then disable or disrupt operations. Wireless packet analyzers, such as AirSnort and WEPcrack, are readily available tools that can be used to gain unauthorized access to networks, putting them at great risk. Unauthorized wireless APs could be deployed by malicious users—tricking legitimate users into connecting to those rogue access points. Malicious users then gain access to sensitive information stored on client machines, including log-ins, passwords, customer information, and intellectual property.

Although WEP is well known and has been widely used, it has inherent flaws in that WEP encryption is fairly easy to crack. As a result, more reliable encryption schemes have been developed, for example, the Wi-Fi Protected Access (WPA). WPA is a security technology for wireless networks that improves on the authentication and encryption features of WEP. In fact, WPA was developed by the networking industry in response to the shortcomings of WEP.

Review Questions

1. What are network access control (NAC) products?
2. Define *authentication*, and give an example of an authentication method.
3. Define *authorization*.
4. What is a firewall? What can it not protect against?
5. Explain the advantage of WPA over WEP.

5.6 Internal Control and Compliance

The **internal control environment** is the work atmosphere that a company sets for its employees. *Internal control (IC)* is a process designed to achieve the following:

- Reliable financial reporting
- Operational efficiency
- Compliance with laws, regulations, and policies
- Safeguarded assets.

INTERNAL CONTROLS NEEDED FOR COMPLIANCE

The Sarbanes-Oxley Act (SOX) is an anti-fraud law. It forces more accurate business reporting and disclosure of GAAP (generally accepted accounting principles) violations, thus making it necessary to find and root out fraud.

Section 302 deters corporate and executive fraud by requiring that the CEO and CFO verify that they have reviewed the financial report, and, to the best of their knowledge, the report does not contain an untrue statement or omit any material fact. To motivate honesty, executive management faces criminal penalties, including long jail terms for false reports. Table 5.6 lists the symptoms, or red flags, of fraud that internal controls can be designed to detect.

Section 805 mandates a review of the Sentencing Guidelines to ensure that "the guidelines that apply to organizations . . . are sufficient to deter and punish organizational criminal conduct." The Guidelines also focus on the establishment of "effective compliance and ethics" programs. As indicated in the Guidelines, a precondition to an effective compliance and ethics program is promotion of "an organizational culture that encourages ethical conduct and a commitment to compliance with the law."

TABLE 5.6 Symptoms of Fraud That Can Be Detected by Internal Controls

- Missing documents
- Delayed bank deposits
- Holes in accounting records
- Numerous outstanding checks or bills
- Disparity between accounts payable and receivable
- Employees who do not take vacations or who go out of their way to work overtime
- A large drop in profits
- A major increase in business with one particular customer
- Customer complaints about double billing
- Repeated duplicate payments
- Employees with the same address or telephone number as a vendor

Among other measures, SOX requires companies to set up comprehensive internal controls. There is no question that SOX, and the complex and costly provisions it requires public companies to follow, has had a major impact on corporate financial accounting. For starters, companies have had to set up comprehensive internal controls over financial reporting to prevent fraud and catch it when it occurs. Since the collapse of Arthur Andersen, following the accounting firm's conviction on criminal charges related to the Enron case, outside accounting firms have gotten tougher with clients they are auditing, particularly regarding their internal controls.

SOX and the SEC are making it clear that if controls can be ignored, there is no control. Therefore, fraud prevention and detection require an effective monitoring system. If the company shows its employees that it can find out everything that every employee does and use that evidence to prosecute that person to the fullest extent of the law, then the feeling that "I can get away with it" drops drastically.

Approximately 85 percent of occupational fraud could have been prevented if proper IT-based internal controls had been designed, implemented, and followed.

SOX requires an enterprise-wide approach to compliance, internal control, and risk management because they cannot be dealt with from a departmental or business-unit perspective. However, protecting against fraud also requires a worldwide approach, as many incidents have indicated, such as the crime server in Malaysia.

WORLDWIDE ANTI-FRAUD REGULATION

Well-executed internal fraud or money-laundering operations can damage the financial sector, capital (money) markets, and, as a result, a nation's economy. A capital market is any market where a government or a company can raise money to finance operations and long-term investment. Examples are the stock and bond markets.

Preventing internal fraud is high on the political agenda, with the Financial Services Authority (FSA) in the United Kingdom and the SEC in the United States both requiring companies to deal with the issue. In May 2007, the FSA fined French investment bank BNP Paribas €350,000 for systems and control failures at its London-based private banking unit that allowed a senior manager to steal €1.4 million from client accounts (Reuters UK, 2007). It was the first time a private bank was fined for weaknesses in anti-fraud systems by the FSA, which warned that it was "raising its game" against firms with lax controls.

Managing risk has become the single most important issue for regulators and financial institutions. Over the years, these institutions have suffered high costs for ignoring their exposure to risk. However, growing research and improvements in IT have improved the measurement and management of risk.

Review Questions

1. Define *internal control*.
2. How does SOX Section 302 deter fraud?
3. List three symptoms or red flags of fraud that can be detected by internal controls.

5.7 Business Continuity and Auditing

Fires, earthquakes, floods, power outages, and other types of disasters hit data centers. Yet business continuity planning and disaster recovery capabilities can be a tough sell because they do not contribute to the bottom line. Compare them to an insurance policy: If and only if a disaster occurs, the money has been well spent. And spending on business continuity preparedness can be an open-ended proposition—there is always more that could be done to better prepare the organization.

Disasters may occur without warning, so the best defense is to be prepared, as described in *IT at Work 5.6*. An important element in any security system is the **business continuity plan,** also known as the disaster recovery plan. Such a plan outlines the process by which businesses should recover from a major disaster. Destruction of all (or most) of the computing facilities can cause significant damage. It is difficult for many organizations to obtain insurance for their computers and information systems without showing a satisfactory disaster prevention and recovery plan.

IT managers need to estimate how much spending is appropriate for the level of risk an organization is willing to accept.

BUSINESS CONTINUITY PLANNING

Disaster recovery is the chain of events linking the business continuity plan to protection and to recovery. The following are some key thoughts about the process:

- The purpose of a business continuity plan is to keep the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan.
- Recovery planning is part of *asset protection.* Every organization should assign responsibility to management to identify and protect assets within their spheres of functional control.
- Planning should focus first on recovery from a total loss of all capabilities.

IT at Work 5.6

Business Continuity and Disaster Recovery

Ninety-three percent of companies that suffer a significant data loss go out of business within five years. Even though business continuity/disaster recovery (BC/DR) is a business survival issue, many managers have dangerously viewed BC/DR as an IT security issue.

Disasters teach the best lessons for both IT managers and corporate executives who have not implemented BC/DR processes. The success or failure of those processes depends on IT, as the following case indicates.

The city of Houston, Texas, and Harris County swung into action by turning Reliant Park and the Houston Astrodome into a "temporary city" with a medical facility, pharmacy, post office, and town square to house more than 250,000 Hurricane Katrina evacuees. Coast Guard Lt. Commander Joseph J. Leonard headed up the operation, drawing on his knowledge of the National Incident Command System. As Leonard explained, ineffective communication between the command staff and those in New Orleans, who could have informed Houston authorities about the number and special needs of the evacuees, caused a serious problem. In addition, agencies and organizations with poor on-scene decision-making authority hampered and slowed efforts to get things done.

Now businesses in hurricane alleys, earthquake corridors, and major cities are deploying BC/DR plans supported with software tools that allow them to replicate, or back up, their mission-critical applications to sites away from their primary data centers. In case of a disaster, companies can transmit vital accounting, project management, or transactional systems and records to their disaster recovery facilities, limiting downtime and data loss despite an outage at the primary location.

Sources: Compiled from Fagg (2006), *Fiber Optics Weekly* (2006), and the Infragard (*infragardconferences.com*).

Discussion Questions: Why might a company that had a significant data loss not be able to recover? Why are regulators requiring that companies implement BC/DR plans?

- Proof of capability usually involves some kind of what-if analysis that shows that the recovery plan is current.
- All critical applications must be identified and their recovery procedures addressed in the plan.
- The plan should be written so that it will be effective in case of disaster, not just in order to satisfy the auditors.
- The plan should be kept in a safe place; copies should be given to all key managers, or it should be available on the intranet. The plan should be audited periodically.

Disaster recovery planning can be very complex, and it may take several months to complete. Using special software, the planning job can be expedited.

Disaster avoidance is an approach oriented toward prevention. The idea is to minimize the chance of avoidable disasters (such as fire or other human-caused threats). For example, many companies use a device called uninterrupted power supply (UPS), which provides power in case of a power outage.

AUDITING INFORMATION SYSTEMS

An **audit** is an important part of any control system. Auditing can be viewed as an additional layer of controls or safeguards. It is considered to be a deterrent to criminal actions, especially for insiders. Auditors attempt to answer questions such as these:

- Are there sufficient controls in the system? Which areas are not covered by controls?
- Which controls are not necessary?
- Are the controls implemented properly?
- Are the controls effective? That is, do they check the output of the system?
- Is there a clear separation of duties of employees?
- Are there procedures to ensure compliance with the controls?
- Are there procedures to ensure reporting and corrective actions in case of violations of controls?

Auditing a Web site is a good preventive measure to manage the legal risk. Legal risk is important in any IT system, but in Web systems it is even more important due to the content of the site, which may offend people or be in violation of copyright laws or other regulations (e.g., privacy protection). Auditing e-commerce is also more complex since, in addition to the Web site, one needs to audit order taking, order fulfillment, and all support systems.

COST-BENEFIT ANALYSIS

It is usually not economical to prepare protection against every possible threat. Therefore, an IT security program must provide a process for assessing threats and deciding which ones to prepare for and which ones to ignore or provide reduced protection against.

Risk-Management Analysis Risk-management analysis can be enhanced by the use of DSS software packages. A simplified computation is shown here:

$$\text{expected loss} = P_1 \times P_2 \times L$$

where:
P_1 = probability of attack (estimate, based on judgment)
P_2 = probability of attack being successful (estimate, based on judgment)
L = loss occurring if attack is successful
Example:

$$P_1 = .02, P_2 = .10, L = \$1{,}000{,}000$$

Then, expected loss from this particular attack is

$$P_1 \times P_2 \times L = 0.02 \times 0.1 \times \$1{,}000{,}000 = \$2{,}000$$

The amount of loss may depend on the duration of a system being out of operation. Therefore, some add duration to the analysis.

Ethical Issues Implementing security programs raises many ethical issues. First, some people are against any monitoring of individual activities. Imposing certain controls is seen by some as a violation of freedom of speech or other civil liberties. A Gartner Group study showed that even after the terrorist attacks of September 11, 2001, only 26 percent of Americans approved of a national ID database. Using biometrics is considered by many to be a violation of privacy.

Handling the privacy versus security dilemma is tough. There are other ethical and legal obligations that may require companies to "invade the privacy" of employees and monitor their actions. In particular, IT security measures are needed to protect against loss, liability, and litigation. Losses are not just financial, but also include the loss of information, customers, trading partners, brand image, and ability to conduct business, due to the actions of hackers, malware, or employees. Liability stems from two legal doctrines: *respondeat superior* and duty of care. *Respondeat superior* holds employers liable for the misconduct of their employees that occurs within the scope of their employment. With wireless technologies and a mobile workforce, the scope of employment has expanded beyond the perimeters of the company.

Under the doctrine of duty of care, senior managers and directors have a fiduciary obligation to use reasonable care to protect the company's business operations. Litigation (lawsuits) stems from failure to meet the company's legal and regulatory duties. According to a *Workplace E-Mail and Instant Messaging Survey* of 840 U.S. companies from the American Management Association and the ePolicy Institute (*epolicyinstitute.com*), more than one in five employers (21 percent) have had employee e-mail and IM subpoenaed in the course of a lawsuit or regulatory investigation.

Review Questions

1. Why do organizations need a business continuity plan?
2. List three issues a business continuity plan should cover.
3. Identify two factors that influence a company's ability to recover from a disaster.
4. What types of devices are needed for disaster avoidance?
5. Explain why business continuity/disaster recovery (BC/DR) is not simply an IT security issue.
6. Why should Web sites be audited?
7. How is expected loss calculated?
8. What is the doctrine of due care?

Key Terms

acceptable use policy (AUP) *131*
adware *135*
application controls *139*
audit *148*
biometric control *140*
business continuity plan *147*
business impact analysis (BIA) *131*
computer systems failures *132*
crime server *133*
data tampering *133*
denial of service (DoS) attack *134*
enterprise risk management (ERM) *128*
environmental hazard *132*
general controls *139*
human errors *132*
intelligent agents *141*
internal control *131*
internal threats *124*
IT security *123*
malware *124*
occupational fraud *136*
Payment Card Industry Data Security Standard (PCI DSS) *129*
phishing *127*
programming attacks *134*
remote administration Trojan (RAT) *134*
retinal scan *141*
service pack *127*
signature *141*
social engineering *133*
spam *135*
spyware *135*
thumbprint or fingerprint *141*
time-to-exploitation *127*
two-factor authentication *143*
virus *134*
wired equivalent privacy (WEP) *145*
worm *134*

Chapter Highlights and Insights

(Numbers Refer to Learning Objectives)

1 Businesses that neglect to consider and implement privacy requirements are subject to enforcement actions, huge lawsuits, penalties, and fines that significantly increase expenses.

1 A company's top line (revenue) suffers when customers discover that their private information has been compromised.

1 Criminals invest considerable effort planning and preparing tactics to bypass company security measures.

2 Responsibility for internal control and compliance rests directly on the shoulders of senior management and the board of directors. SOX and other anti-fraud regulations force better business reporting and disclosure of GAAP violations, thus making it necessary and easier to find and root out fraud.

2 The chief privacy officer (CPO) and chief security officer (CSO) are corporate-level positions demonstrating the importance and changing role of IT security in organizations.

3 Data, software, hardware, and networks can be threatened by internal and external hazards.

3 One of the biggest mistakes managers make is underestimating vulnerabilities and threats.

3 Computer criminals are increasingly profit-driven.

4 The risk exposure model for digital assets has five factors: the asset's value to the company, attractiveness to criminals, legal liability attached to its loss or theft, impact on business performance, and likelihood of a successful attack.

4 The consequences of wireless attacks include data theft, legal and recovery expenses, tarnished image, lost customers, and disrupted operations due to loss of network service.

5 With two-factor authentication, two types of information are used to verify the user's identity, such as passwords and biometrics.

5 Biometric controls are used to identify users by checking physical characteristics such as a fingerprint or voice-print.

5 Encryption is extremely important for confidential data that is sent or stored.

6 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as a process designed to provide reasonable assurance of effective operations and reliable financial reporting.

6 There is no such thing as small fraud, only large fraud that was detected and stopped early.

7 Disaster recovery planning is an integral part of effective internal control and security management.

7 Business continuity planning includes data backup and a plan for what to do when disaster strikes.

7 Protecting critical infrastructures, including energy, IT, telecommunications, and transportation sectors, is a key part of national security.

7 A large range of IT security tools, including intelligent agents and anti-fraud measures, help defend against counterterrorist activities.

Questions for Discussion

1. Many firms concentrate on the wrong questions and end up throwing a great deal of money and time at minimal security risks while ignoring major vulnerabilities. Why?
2. How can the risk of occupational fraud be decreased?
3. Why should information control and security be of prime concern to management?
4. Compare the computer security situation with that of insuring a house.
5. Explain what firewalls protect and what they do not protect. Why?
6. Why is cybercrime expanding rapidly? Discuss some possible solutions.
7. Why are authentication and authorization important in e-commerce?
8. Some insurance companies will not insure a business unless the firm has a computer disaster recovery plan. Explain why.
9. Explain why risk management should involve the following elements: threats, exposure associated with each threat, risk of each threat occurring, cost of controls, and assessment of their effectiveness.
10. Discuss why the Sarbanes-Oxley Act focuses on internal control. How does that focus influence infosec?
11. Discuss the shift in motivation of criminals.

Exercises and Projects

1. A critical problem is assessing how far a company is legally obligated to go. Since there is no such thing as perfect security (i.e., there is always more that you can do), resolving these questions can significantly affect cost.
   a. When are a company's security measures sufficient to comply with its obligations? For example, does installing a firewall and using virus detection software satisfy a company's legal obligations?
   b. Is it necessary for an organization to encrypt all of its electronic records?

2. The SANS Institute publishes the Top 20 Internet Security Vulnerabilities (*sans.org/top20*).
   a. Which of those vulnerabilities are most dangerous to financial institutions?
   b. Which of those vulnerabilities are most dangerous to marketing firms?
   c. Explain any differences.
3. Access the Anti-Phishing Working Group Web site (*antiphishing.org*) and download the most recent Phishing Activity Trends Report.
   a. Describe the recent trends in phishing attacks.
   b. Explain the reasons for these trends.
4. Assume that the daily probability of a major earthquake in Los Angeles is .07 percent. The chance of your computer center being damaged during such a quake is 5 percent. If the center is damaged, the average estimated damage will be $1.6 million.
   a. Calculate the expected loss (in dollars).
   b. An insurance agent is willing to insure your facility for an annual fee of $15,000. Analyze the offer, and discuss whether to accept it.
5. The theft of laptop computers at conventions, hotels, and airports is becoming a major problem. These categories of protection exist: physical devices (e.g., *targus.com*), encryption (e.g., *networkassociates.com*), and security policies (e.g., at *ebay.com*). Find more information on the problem and on the solutions. Summarize the advantages and limitations of each method.
6. Should an employer notify employees that their usage of computers is being monitored? Why or why not?
7. Twenty-five thousand messages arrive at an organization each year. Currently there are no firewalls. On average, there are 1.2 successful hackings each year. Each successful hack attack results in loss to the company of about $130,000. A major firewall is proposed at a cost of $66,000 and a maintenance cost of $5,000. The estimated useful life is three years. The chance that an intruder will break through the firewall is .0002. In such a case, the damage will be $100,000 (30%), or $200,000 (50%), or no damage. There is an annual maintenance cost of $20,000 for the firewall.
   a. Should management buy the firewall?
   b. An improved firewall that is 99.9988 percent effective and that costs $84,000, with a life of three years and annual maintenance cost of $16,000, is available. Should this one be purchased instead of the first one?

Group Assignments and Projects

1. Each group is to be divided into two parts. One part will interview students and businesspeople and record the experiences they have had with computer security problems. The other part of each group will visit a computer store (and/or read the literature or use the Internet) to find out what software is available to fight different computer security problems. Then each group will prepare a presentation in which they describe the problems and identify which of the problems could have been prevented with the use of commercially available software.
2. Create groups to investigate the latest development in IT and e-commerce security. Check journals such as *cio.com* (available free online), vendors, and search engines such as *techdata.com* and *google.com.*
3. Research a botnet attack. Explain how the botnet works and what damage it causes. What preventive methods are offered by security vendors?

Internet Exercises

1. Visit *cert.org* (a center of Internet security expertise). Read one of the recent Security Alerts or CERT Spotlights and write a report.
2. Visit *cert.org/csirts/services.html.* Discover the security services a CSIRT can provide in handling vulnerability. Write a summary of those services.
3. Visit *dhs.gov/dhspublic* (Department of Homeland Security). Search for an article on E-Verify. Write a report on the benefits of this verification program and who can benefit from it.
4. Visit *first.org* (a global leader in incident response). Find a current article under "Global Security News" and write a summary.
5. Visit *issa.org* (Information Systems Security Association) and choose a Webcast to listen to—one concerned with systems security. Write a short opinion essay.
6. Visit *wi-fi.org* (Wi-Fi Alliance) and discover what its mission is. Report on what you think about its relevance in the overall wireless security industry.
7. Visit *securitytracker.com* and select one of the vulnerabilities. Describe the vulnerability, its impacts, its cause, and the affected operating system.
8. Visit *cio.com* and search for a recent article on security, privacy, or compliance. Write a brief summary of the article.
9. Enter *scambusters.org*. Find out what the organization does. Learn about e-mail and Web site scams. Report your findings.
10. Enter *epic.org/privacy/tools.html* and examine one of the following groups of tools: snoop proof e-mail, encryption, or firewalls. Discuss the security benefits.
11. Access the Web sites of any three major antivirus vendors (e.g., *symantec.com*, *mcafee.com*, and *antivirus.com*). Find out what the vendors' research centers are doing. Also download VirusScan from McAfee and scan your hard drive with it.
12. Research vendors of biometrics. Select one vendor and discuss three of its biometric devices or technologies. Prepare a list of major capabilities. What are the advantages and disadvantages of its biometrics?

BUSINESS CASE

NEC's Weak Internal Controls Contribute to NASDAQ Delisting

In September 2007, the Japan-based electronics company NEC announced that it could not complete the financial analysis it was required to file with the SEC (Securities and Exchange Commission). SEC filings are mandatory for every company listed on any U.S. stock exchange. The key reason NEC could not properly prepare its financial statements stemmed from at least two frauds that had been committed by NEC employees from 1999 through 2005. Weak internal controls allowed the frauds to continue for years.

Weak Internal Control Enables Uncontrolled Fraud

Fraud #1: In 2006, NEC had to restate its earnings for five prior years after discovering that a 50-year-old manager/engineer had been fabricating business deals. His bogus deals inflated sales by 36.3 billion yen ($311 million). The false transactions enabled him to embezzle tens of millions of yen, which he spent on entertainment. NEC discovered that he had made a series of false transactions from March 2002 to December 2005 in the semiconductor production department at NEC Engineering (NECE) Ltd., a wholly owned subsidiary. The fraudulent transactions amounted to nearly 10 percent of NECE's sales between 2001 and 2004.

The NECE manager, who in March 2002 anticipated poor performance in his department, convinced a client company to make up bogus transactions. He went on to make up about 200 orders and payments by forging order and estimation forms. He allowed firms that pretended to have received deliveries to make payments to NECE for items that were never delivered.

NEC filed criminal actions against the manager, reviewed its internal control system, and strengthened the administration of those controls. The company had not been able to detect the fraud because the manager involved had been in a position to prepare all of the necessary documents to make the fictitious trades look real. There was no separation of duties, oversight, surprise audit, or forced vacation time, which might have caught the fraud. For more information on preventing and detecting fraud, see *ACFE.com* and *AICPA.org*. Despite an internal investigation, it did not become clear how the manager was able to falsify all of the data and payments.

"NEC deeply regrets the occurrence of these fraudulent transactions at a time when strengthening of corporate compliance and the improvement of internal controls is being strongly sought after, and sincerely apologizes for any inconvenience caused," the company said in the filing. A NEC spokesperson stated, "We don't expect a big impact" from the accounting fraud. They were wrong. Another fraud was discovered soon afterwards.

Fraud #2: NEC discovered fraud carried out by 10 employees during the seven-year period ending March 31, 2006. The fraudulent transactions amounted to roughly $18 million. The 10 NEC employees convinced contractors to inflate or create fictitious orders to their subcontractors, such as orders for software, maintenance, and installation. This resulted in the fraudulent outflow of NEC's money through these contractors. The 10 employees received approximately 500 million yen ($4.1 million) in kickbacks from the subcontractors and used it for their own personal purposes, such as on entertainment.

Internal Controls Implemented

The company explained that fraud was not discovered for a prolonged time because the information systems enabled validation of the orders and confirmation by the same employees who made the orders. In response to its internal control deficiencies, NEC established an internal control system by which confirmation is carried out by a third-party administrative division. Other internal controls have been implemented to meet SOX compliance mandates.

Outcome

The frauds have had a very real and long-lasting effect on NEC's standing with the regulatory authorities. NEC released the following cautionary note in its April 21, 2006, financial forecast: "As announced on March 22, 2006, NEC had to restate its earnings in its financial statements for past fiscal years as a result of the fraud and other revisions based on U.S. generally accepted accounting principles (U.S. GAAP)."

In May 2007, NEC disclosed that it was at risk of losing its listing on the NASDAQ stock market because of its long-overdue SEC filings. In September 2007, after requesting multiple extensions for financial filing from NASDAQ, NEC finally admitted defeat. With sincere apologies to investors everywhere, NEC said its financial statements from 2000 to 2006 were now unreliable and that it would accept delisting in New York.

Sources: Compiled from NEC (2006), Nakamoto (2006), Taylor (2007a, 2007b).

Questions

1. What might have been some of the indicators that the NECE manager/engineer was committing fraud? What type of information systems could have helped to detect the fraud?
2. Use an Internet browser to do a search on the term "restatement of earnings." Explain the results.
3. What types of internal controls might have prevented or detected the fraud?

PUBLIC SECTOR CASE

Blue Cross Mistake Releases Data of 12,000 Members

In April 2010, Blue Cross & Blue Shield of Rhode Island (BCBSRI) announced that personal information belonging to approximately 12,000 BlueCHiP for Medicare members was inadvertently contained in a filing cabinet donated with other surplus office furniture to a local nonprofit organization.

The filing cabinet contained BlueCHiP for Medicare Health Surveys, which included names, addresses, telephone numbers, Social Security numbers, Medicare identification numbers, and medical information.

BCBSRI's Privacy Officer immediately retrieved the documents, began an investigation, and notified appropriate federal and state authorities of the incident, including the U.S. Centers for Medicare and Medicaid Services, the U.S. Department of Health and Human Services Office for Civil Rights, the Rhode Island Attorney General, and the Rhode Island Health Insurance Commissioner.

In a letter to the approximately 12,000 affected BlueCHiP for Medicare members, BCBSRI apologized for the error, notified them of a special hotline available, and offered each affected member free credit monitoring for one year.

Due to the swift action of the nonprofit in notifying BCBSRI, it was believed there was little chance that member information was misused.

BCBSRI's internal investigation revealed that the disclosure was the result of the failure of certain employees to adhere to the company's strict information-handling policies and procedures. As a result of this breach, those responsible for the data breach were disciplined, and several of them were fired.

While the disclosure appears to have been contained, out of an abundance of caution, BCBSRI is providing the affected BlueCHiP for Medicare members with free credit monitoring, assistance in every aspect of identity theft protection, and an identity protection product guarantee for one year, provided by ConsumerInfo.com, Inc., an Experian company. Members were given direct access to immediately activate their protection. Among other services, members will have free access to:

- A copy of their Experian credit report
- Daily monitoring and timely alerts of any key changes to their credit reports
- Daily scanning of the Internet of their Social Security, credit card, and debit card information to better protect against potential fraud
- Assistance with the cancellation of their credit and debit cards
- Toll-free access to a dedicated team of fraud resolution representatives who will help investigate each incident, contact credit grantors to dispute charges, close accounts, if necessary, and compile documents and contact all relevant government agencies
- A $1 million product guarantee to reimburse them from identity theft–related losses such as lost wages, legal fees, and stolen funds should the protection fail

Management announced that they will learn from this incident and take all appropriate steps to maintain the trust that members have in their privacy and security standards.

Sources: Compiled from *PHIprivacy.net* (2010), *Databreaches.net* (2010), and *BSBCRI.com*

Questions

1. Explain the reasons for the data breach.
2. What types of costs did BSBCRI incur because of the breach?
3. Why did BSBCRI notify government agencies immediately?
4. To what extent could this data breach have been prevented?
5. Why did BSBCRI take such fast and thorough action to protect its members?
6. Why was restoring trust so important to the company?
7. What would you recommend BSBCRI do to prevent another infosec incident?

ANALYSIS USING SPREADSHEETS

Estimating Investments in Antispam Protection

It is difficult for companies to assess the costs of not implementing infosec defenses. Most companies do not do a proper postmortem, or, if they do, they have no idea what to include in the analysis. Cost estimates may include the soft costs (i.e., hard to quantify costs) of diverting the IT department from a strategic project, lost sales, and customer attrition, or take a minimalist approach that only includes recovery costs. Rather than a single point estimate, several estimates can be made using a DSS to support the decision regarding infosec investments.

Using the model for estimating the cost of spam shown in Figure 5.10, design a DSS using Excel or other spreadsheet software. Enter the formulas as shown in the figure. Then enter data to calculate three scenarios—optimistic, realistic, and pessimistic. This is your cost analysis using a range of estimates.

Write a report that includes your DSS model (spreadsheet), showing the results. Estimate how much the company should invest in antispamware. Explain your answer.

Model for Estimating the Cost of Spam (Optimistic, Pessimistic, and Realistic Estimates)

	Labor Costs	Optimistic	Pessimistic	Realistic
A	Number of employees	5	10	8
B	Average employee annual salary	$ 50,000	$ 70,000	$ 60,000
C	Average number of working days/year	245	250	248
D	Average number of emails per day per employee	25	50	38
E	Percentage of emails that are spam	20%	40%	30%
F	Average time to process each one (seconds)	5	10	8
	Technical Costs			
G	Cost of bandwidth per year per site			–
H	Number of sites			–
I	Annual cost of bandwidth (G*H)			–
J	Percentage of bandwidth used by email			–
K	Total annual cost of bandwidth used by spam (I*J)			–
L	Cost of email storage per GB			–
M	Size of average spam, in KB			–
N	Total annual cost of storing spam (A*C*E*M*0.000008) (storage cost/KB)			–
O	Support costs per user per year			–
P	Percentage attributable to spam			–
Q	Total support cost of spam (O*P*A)			–
R	Number of email servers			–
S	Hardware cost (R*$5,000 per server)			–
T	% of email server capacity used by spam			–
U	Spam cost in hardware (S*T)			–
V	Average annual cost of time lost per employee ((E*F)/60*C)*(B/((C*8)*60))			–
W	Total productivity cost of spam (A*V)			–
	Anti-Spam Costs			
X	Annual cost of anti-spam software & tuning			–
Y	Percentage of spam stopped by filters			–
Z	Total cost of spam (K+N+Q+U+W)			–
	Totals			
AA	Total cost after filtering (Z*(1-Y)+X)			–
BB	Total savings (Z-AA)			–
CC	Total percentage cost savings (BB/Z)			–

Figure 5.10 Model for estimating cost of spam.

Resources on the Book's Web Site

More resources and study tools are located on the Student Web Site and on WileyPLUS. You'll find additional chapter materials and useful Web links. In addition, self-quizzes that provide individualized feedback are available for each chapter.

Case for Chapter 5 is available at wiley.com/college/turban:

5.1 $55 Million Data Breach at ChoicePoint

References

Aftergood, S., "Former Official Indicted for Mishandling Classified Info," *FAS*, April 15, 2010. *fas.org/blog/secrecy/2010/04/drake_indict.html*

Altman, H., "Jihad Web Snares Online Shops, Buyers," *Tampa Tribune*, February 20, 2006.

Antilla, S., "Red Flags Were There All Along; Suspicious Activities Largely Unquestioned." *The Gazette* (Montreal), December 16, 2008.

Appelbaum, B., and D. S. Hilzenrath. "SEC Ignored Credible Tips About Madoff, Chief Says." *Washington Post*, December 17, 2008.

Barrett, L., "HSBC Confirms Massive Database Security Breach," *eSecurityPlanett.com*, March 11, 2010. *esecurityplanet.com/features/article.php/3870071/HSBC-Confirms-Massive-Database-Security-Breach.htm*

"Blue Cross Mistake Releases Personal Info of 12K Members," April 16, 2010. *databreaches.net/*

Chew, R., "A Madoff Whistle-Blower Tells His Story." *Time.* February 4, 2009. *time.com/time/business/article/0,8599,1877181,00.html*

Edwards, J., "The Rise of Botnet Infections," *Network Security Journal*, February 13, 2008. *networksecurityjournal.com/features/botnets-rising-021308*

Fagg, S., "Continuity for the People," *Risk Management Magazine,* March 2006.

Fiber Optics Weekly Update, "Telstra Uses NetEx Gear," January 13, 2006.

Gold, L., "Forensic Accounting: Finding the Smoking E-Mail; E-Discovery Is Now a Critical Part of Forensics—and of Firm Policy," *Accounting Today,* 22(8), May 5, 2008.

Higgins, K. J., "Crime Server Discovered Containing 1.4 Gigabytes of Stolen Data," *Dark Reading,* May 6, 2008. *darkreading.com/document.asp?doc_id=153058*

HSBC-RI (Blue Shield Blue Cross of Rhode Island), "Important Notice for BlueCHiP for Medicare Members," April 16, 2010. *bcbsri.com/BCBSRIWeb/about/newsroom/news_releases/2010/MemberInfoBreach.jsp*

Kaplan, D., "ChoicePoint Settles Lawsuit over 2005 Breach," *SC Magazine*, January 28, 2008. *scmagazineus.com/ChoicePoint-settles-lawsuit-over-2005-breach/article/104649/*

Leyden, J., "Swiss HSBC Data Breach Victim Count Trebles," *Enterprise Security*, April 15, 2010.

McGlasson, L., "'Crime Server' Found with Thousands of Bank Customer Records: FBI Investigating Breach Affecting 40 Global Institutions," *Bank Info Security,* May 7, 2008. *bankinfosecurity.com/articles.php?art_id=846*

Nakamoto, M., "NEC to Restate Earnings After Fraud," *Financial Times*, March 23, 2006.

NEC, "Revision of NEC Corporation's Financial Forecast for Fiscal Year Ended March 31, 2006." *nec.co.jp/press/en/0604/2101.html*

PHIPrivacy.net, Blue Cross Mistake Releases Personal Info of 12K Members," April 16, 2010.

Quinn, J. "On the Trail of Madoff's Missing Billions." *Sunday Telegraph* (London), January 18, 2009.

Reuters UK, "BNP Paribas Fined for UK Anti-Fraud Failings," May 10, 2007. *uk.reuters.com/article/UK_SMALLCAPSRPT/idUKWLA850120070510*

Spangler, T., "What You Can Learn from the VA's Snafu," *Baseline*, May 24, 2006.

Taylor, C., "NEC Employees Behind $18M Fraud Scheme," *EDN*, May, 29, 2007a, *dn.com/article/CA6447014.html*

Taylor, C., "NEC Stock Faces Nasdaq Delisting," *EDN*, September 21, 2007b. *edn.com/index.asp?layout=article&articleid=CA6480624*

U.S. Department of State, *state.gov,* 2008.

Wolfe, D., "Security Watch," *American Banker,* June 2, 2006.