Part II Data and IT Infrastructure

Chapter 5 Securing the Enterprise and Business Continuity

Learning Objectives

After studying this chapter, you will be able to:

1. Recognize the business and financial value of information security.

2. Recognize IS vulnerabilities, threats, attack methods, and cybercrime symptoms.

3. Describe the factors that contribute to risk exposure and the methods to mitigate them.

4. Explain key methods of defending information systems, networks, and wireless devices.

5. Describe internal control and fraud and the related legislation.

6. Understand business continuity and disaster recovery planning methods.

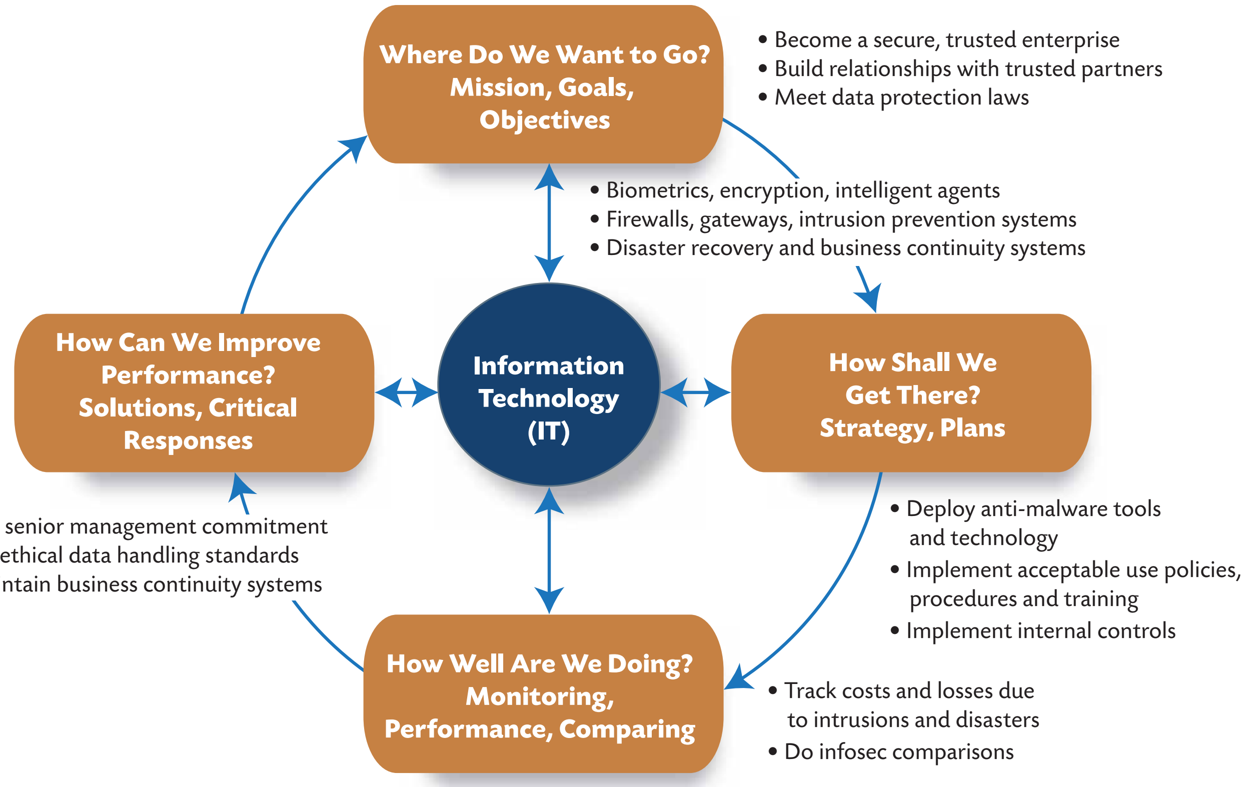
7. Discuss the role of IT in defending critical infrastructures.

Integrating *IT*

ACC FIN MKT OM HRM IS

IT-PERFORMANCE MODEL

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 of staying ahead of deliberate attacks, viruses and other malware infections, and unintentional errors. Managers have a fiduciary responsibility to protect confidential data that they collect and store. Yet, according to research published by Computer Economics (*computereconomics.com*), many companies of all sizes fail to invest in basic security management best practices, such as IT security training for their employees or the auditing of computers to ensure that unauthorized programs or content are not present. To comply with federal, state, and foreign laws, companies must invest in IT security to protect their data, other assets, the ability to operate, and net income.


Where Do We Want to Go? Mission, Goals, Objectives
• Become a secure, trusted enterprise
• Build relationships with trusted partners
• Meet data protection laws
• Biometrics, encryption, intelligent agents
• Firewalls, gateways, intrusion prevention systems
• Disaster recovery and business continuity systems
How Can We Improve Performance? Solutions, Critical Responses
Information Technology (IT)
How Shall We Get There? Strategy, Plans
• Get senior management commitment
• Set ethical data handling standards
• Maintain business continuity systems
• Deploy anti-malware tools and technology
• Implement acceptable use policies, procedures and training
• Implement internal controls
How Well Are We Doing? Monitoring, Performance, Comparing
• Track costs and losses due to intrusions and disasters
• Do infosec comparisons

The business performance management cycle and IT model.

$55 MILLION DATA BREACH AT CHOICEPOINT

ETHICS ACC FIN HRM IS OM GOV

ChoicePoint is a leading data broker and credentialing service. It maintains 19 billion public records on more than 220 million U.S. citizens. The company buys personal data, including names, Social Security numbers, birthdates, employment data, and credit histories, and then sells the data to businesses and government agencies. Marketing, human resources, accounting, and finance departments rely on ChoicePoint's data for customer leads, background checks, and verification. Roughly, 70 percent of ChoicePoint's revenue is generated by selling consumer records for insurance claim verifications and workplace background screenings.

ChoicePoint was exposing the data to risk by ignoring its policy to verify that potential customers were legitimate before selling data. Disaster was foreseeable. In early 2000, without doing an adequate background check, ChoicePoint provided the hackers with customer accounts, which they used to illegally access databases and steal confidential data. By May 2008, that security lapse had cost the company over $55 million in fines, compensation to potential victims of identity theft, lawsuit settlements, and legal fees. Then in June 2008, the company also paid $10 million to settle a class action lawsuit.

Disclosing the Problem Publicly

On February 15, 2005, ChoicePoint reported that personal and financial data of 145,000 individuals had been "compromised." All of the individuals were at risk of identity theft after Olatunji Oluwatosin, a Nigerian national living in California, had pretended to represent several legitimate businesses. Ironically, Oluwatosin's credentials had not been verified, which enabled him to set up over 50 bogus business accounts. Those accounts gave him access to databases containing personal financial data. Oluwatosin was arrested in February 2005, pleaded guilty to conspiracy and grand theft, and was sentenced to 10 years in prison and fined $6.5 million. The state and federal penalties facing ChoicePoint were much larger.

Privacy and antifraud laws required that ChoicePoint disclose what had happened. California's privacy breach legislation requires that residents be informed when personal information has been compromised. Outraged Attorneys General in 44 states demanded that the company notify every affected U.S. citizen. At the federal level, ChoicePoint was charged with multiple counts of negligence for failing to follow *reasonable* information security practices. In 2005, the company was hit with the largest fine in Federal Trade Commission (FTC) history—$15 million. The FTC charged ChoicePoint with violating:

- The Fair Credit Reporting Act (FCRA) for furnishing credit reports to subscribers who did not have a permissible purpose to obtain them, and by not maintaining reasonable procedures to verify their subscribers' identities
- The FTC Act for false and misleading statements about privacy policies on its Web site

On March 4, 2005, in what was a first for a publicly held company, ChoicePoint filed an 8-K report with the SEC warning shareholders that revenue would be adversely affected by the data breach. In January 2006, with the public announcement of the extent of the fines, ChoicePoint's stock price plunged, as shown in Figure 5.1.

The Solution

When a company violates SEC, federal, or state laws, the solution to their problem is going to be dictated to them. The solution to ChoicePoint's risk exposure was mandated by the FTC. The company had to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes. In addition, the FTC ordered ChoicePoint to establish and maintain a comprehensive information security program and to obtain audits by an independent third-party security professional biyearly until 2026. To reassure stakeholders, ChoicePoint hired Carol DiBattiste, the former deputy administrator of the Transportation Security Administration, as chief privacy officer (CPO).

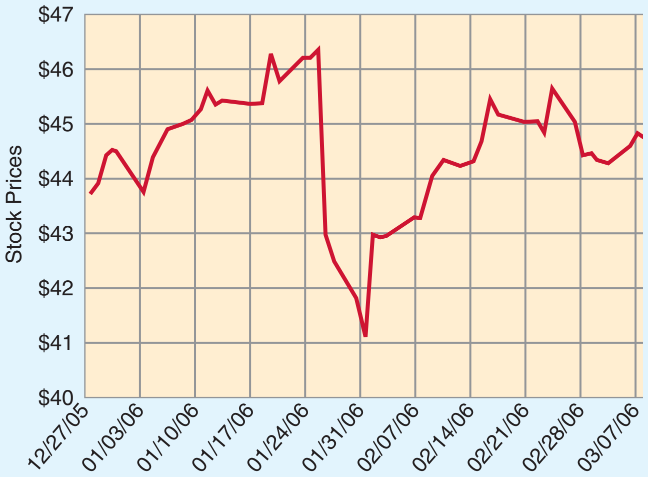


Figure 5.1 Impact of data breach on ChoicePoint's stock price.

The Results

ChoicePoint reformed its business practices and data security measures, which were too lax relative to its risk exposure. The company had to stop putting risky business practices that focused on short-term revenues ahead of long-term profitability. This business decision is a necessary and ethical trade-off.

ChoicePoint's data breach brought businesses' security policies to national attention. It signaled the need for improved corporate governance (see *corpgov.net*). Although there is no generally accepted definition, **corporate governance** refers to the rules and processes ensuring that the enterprise adheres to accepted ethical standards, best practices, and laws. Companies that collect sensitive consumer information have a responsibility to keep it secure. Together with high-profile frauds and malware, data breaches have triggered an increase in laws and government involvement to hold companies and their management accountable for lapses in governance. Yet, since ChoicePoint's record-setting data breach, many other infosec incidents and data thefts have occurred.

Sources: Compiled from *ftc.gov, Gross* (2005), Kaplan (2008), Mimoso (2006), and Scalet (2005).

Lessons Learned from This Case

Every enterprise has information assets that criminals worldwide attempt to steal. IT security risks are business risks. **IT security** refers to the protection of information, communication networks, and traditional and e-commerce operations to assure their confidentiality, integrity, availability, and authorized use. The purpose is to defend against operational risk and disruptions, outraged customers, and financial loss and liability. **Operational risk** is the risk of any loss resulting from inadequate or failed internal processes, people, systems, or external events. 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.

In this chapter we begin with an overview of enterprisewide security issues. We discuss technologies, such as firewalls and malware, internal controls, information assurance, and the COBIT framework. We introduce a risk exposure model for identifying what to protect and how much to invest in that protection. We describe major threats and types of fraud—and how they have increased the incidence of spam, bots, and phishing. Note, we use the term information security (or *infosec*, for short) to refer broadly to the security of data, networks, applications, communications, and everything digital needed for the enterprise to function.

5.1 Data and Enterprise Security Incidents

Until 2002, infosec was mostly a technical 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. Cleanup costs after a single incident are already into the tens or hundreds of millions of dollars. For up-to-date information and blogs on spyware, see SpywareGuide, a public reference site, at *spywareguide.com*.

INFOSEC THREATS AND INCIDENTS

Threats to infosec range from high-tech exploits to gain access to a company's networks and databases to non-tech tactics to steal laptops and whatever 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.

Controlling physical and remote access to proprietary systems and information continues to present IT security challenges. A vast majority of data breaches involve some sort of insider error or action, either intentional or unintentional. (These threats are discussed in Section 5.2.) Threats from employees, referred to as **internal threats,** are a major hurdle largely due to the huge number of ways available to an employee to carry out malicious activity. The following internal incidents could have been prevented if stringent infosec policies and defenses had been enforced. They also point out that victims of breaches are often third parties, such as customers, patients, social network users, credit card companies, and shareholders.

- 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 January 2007, TJX Companies disclosed that data from 100 million credit and debit cards had been stolen by hackers starting in July 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

TABLE 5.1 IT Security Terms

Term	Definition
Threat	Something or someone that may result in harm to an asset
Vulnerability	Weakness that threatens the confidentiality, integrity, or availability of an asset
Risk	Probability of a threat exploiting a vulnerability
CIA triad (confidentiality, integrity, availability)	The three main principles of IT security
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
Exploit	A tool or technique that takes advantage of a vulnerability
Access control	Security feature designed to restrict who has access to a network, IS, or data. Access to resources on a computer is restricted using a logical or physical control designed to protect against unauthorized entry or use
Countermeasure	Safeguard implemented to mitigate (lessen) risk
Audit	The process of generating, recording, and reviewing a chronological record of system events to ascertain their accuracy
Encryption	Transforming 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	Malicious software, such as a virus, worm, or Trojan horse
Biometrics	Methods to identify a person based on a biological feature, such as a fingerprint
Perimeter security	Security measures to ensure that only authorized users gain access to the network
Endpoint security	Security measures to protect the *end points*, such as desktops and laptops, in the enterprise
Firewall	A method (hardware or software) of guarding 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 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 (Bot network)	A network of hijacked computers that are controlled remotely—typically to launch spam or spyware. Also called software robots. Bot networks are linked to a range of malicious activity, including identity theft and spam.

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, birthdates, 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 it 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.

For Further Exploration: 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?

to prevent unauthorized access to the sensitive, personal customer information. The total cost of the data breach was an estimated $197 million. To compare this cost to TJX's financials, see *finance.google.com/finance?fstype=ia&q=NYSE:TJX*.

- Three medical data breaches occurred in May 2008. Unauthorized peer-to-peer (P2P) file-sharing led to a data breach at Walter Reed Army Medical Center that exposed the personal data of 1,000 patients. Patients at Staten Island University Hospital in New York were told that a computer with their medical records was stolen. Information on patients of the University of California San Francisco Medical Center was accidentally made accessible on the Internet.
- In February 2008, security company Symantec (*symantec.com*) warned of a critical flaw in the ActiveX control of image uploaders, which had been distributed to Facebook and MySpace users. Hackers could exploit the flaw to install malicious code on users' computers and take control of them. As a result, the Canadian legal professionals filed charges accusing Facebook of 22 privacy violations. Facebook is coming under increased attack by spammers and phishers, according to the company's security chief.
- In June 2008, Microsoft warned Windows XP and Vista users who had installed Safari on their machines that they were at risk from a blended attack and malicious code.
- In January 2008, T. Rowe Price began notifying 35,000 clients that their names and Social Security numbers might have been compromised. The breach stemmed from the December 2007 theft of computers from the offices of a third-party services provider, which was preparing tax forms on behalf of T. Rowe Price.
- Names, e-mail and home addresses, and phone numbers of an estimated 1.6 million job seekers were accessed from *Monster.com's* résumé database in August 2007. Though widely described as a hacking, the data were actually accessed by attackers using legitimate usernames and passwords, possibly stolen from professional recruiters or human resources personnel who were using *Monster.com* to look for job candidates.
- 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. The disks disappeared in transit to the U.K. National

Audit Office. Analyst firm Gartner Inc. estimated that the closure of compromised accounts and establishment of new ones cost British banks about $500 million.

As the preceding examples illustrate, infosec breaches harm profitability and customer relations. Since January 2005, the Privacy Rights Clearinghouse has identified more than 215 million records belonging to U.S. residents that have been compromised due to a security breach. Plus, a 2007 study conducted by the Ponemon Institute determined that the total average cost for exposed data grew to $197 per compromised record, an 8 percent increase since 2006 and 43 percent increase since 2005.

INCREASING VULNERABILITY

Information resources are distributed throughout the organization and beyond because Internet and wireless technologies extend and connect organizational boundaries. The **time-to-exploitation** of today's most sophisticated spyware and mobile viruses has shrunk from months to days. Time-to-exploitation is the elapsed time between when a vulnerability is discovered and when it is exploited. IT staff have ever-shorter timeframes to find and fix flaws before being compromised by an attack.

New vulnerabilities are continuously being found in operating systems, applications, and wired and wireless networks. Microsoft, for example, releases **service packs** (see *support.microsoft.com/sp*) to update and patch vulnerabilities in its operating systems, including Vista, and other software products, including Office 2007. Left undetected or unprotected, vulnerabilities provide an open door for IT attacks—and business disruptions and their financial consequences. Despite even the best defenses, infosec incidents can still occur. For an example, read how UBS PaineWebber's business operations were shut down by malicious code planted by an employee in Online Minicase 5.1.

With data resources available on demand 24/7, companies benefit from the opportunities for productivity improvement and data sharing with customers, suppliers, and business partners in their supply chain. IT on demand is an operational and competitive necessity for global companies, but the vulnerabilities it creates require strong IT governance as described in *A Closer Look 5.1.*

GOVERNMENT REGULATION

Data must be protected against existing and future attack schemes, and defenses must satisfy ever-stricter government and international regulations. SOX, Gramm-Leach-Bliley Act (GLB), Federal Information Security Management Act (FISMA), and

A Closer Look 5.1

IT Governance Best Practices

ACC FIN HRM IS OM ETHICS

Five IT governance requirements to maximize value and security of information assets are:

1. Align IT strategy with the business strategy.
2. Disseminate strategy, goals, and policies down into the enterprise.
3. Measure and monitor IT's performance.
4. Provide organizational structures that facilitate the implementation of strategy, goals, and policies.
5. Insist that an IT control framework be adopted, implemented, and enforced.

Addressing these issues is at the core of IT governance. To help organizations successfully meet business challenges and regulatory requirements, the IT Governance Institute (*itgi.org*) publishes *Control Objectives for Information and Related Technology* (COBIT). See *isaca.org* to download a copy of COBIT. COBIT 4.1, issued in July 2007, is an internationally applicable and 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. 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 actually implement them.

One Sarbanes-Oxley Act (SOX) mandate is providing evidence that financial applications and supporting systems are secured so financial reports can be trusted. This requires that IT security managers work with business representatives to do a risk assessment to identify which systems depend on technical controls rather than on business process controls. All IT projects should have the same objectives, which are based on:

- The higher principle of economic use of resources (effectiveness and efficiency)
- The principle of legality (meets legal requirements)
- Accounting standards regulations, which are integrity, availability, and reliability

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 II (global financial services) all mandate the protection of personal data. The director of the FTC's bureau of consumer protection warned that the agency would bring enforcement action against small businesses lacking adequate policies and procedures to protect consumer data.

INDUSTRY STANDARDS

Industry groups imposed 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 is required for all members, merchants, or service providers that store, process, or transmit cardholder data. In June 2008, Section 6.6 of the PCI DSS went into full effect. 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 actually help curb 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.

INFORMATION SYSTEMS BREAKDOWNS BEYOND COMPANY CONTROL

Some types of incidents are beyond a company's control. 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 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 attacks. Mission-critical systems and

Figure 5.2 Lower Manhattan, the most communications-intensive real estate in the world. *(Photo courtesy of Verizon Communications. Used with permission.)*

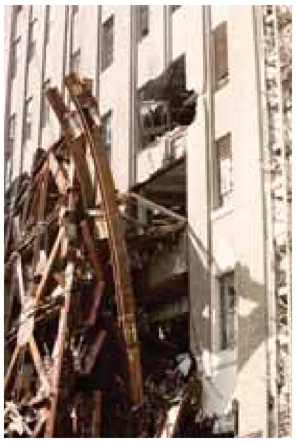


Figure 5.3 Verizon's Central Office (CO) at 140 West St. harpooned by steel girders. *(Photo courtesy of Verizon Communications. Used with permission.)*

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 at 140 West Street, directly across from the WTC—suffered massive structural damage. This CO, which was one of the largest and most complex telecommunications facilities in the world, was harpooned by huge steel girders, as shown in Figure 5.3. 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.

LEADING FACTORS IN INFOSEC INCIDENTS: MISTAKES, MALFUNCTIONS, MISUNDERSTANDINGS, AND MOTIVATION

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 key factors:

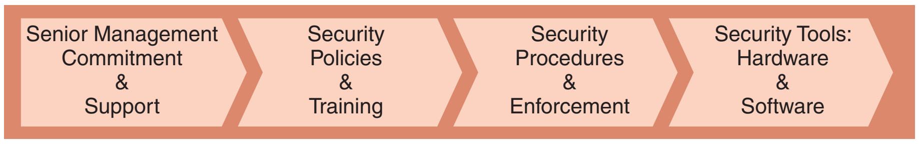
- Mistakes (human error)
- Malfunctioning systems
- Misunderstanding the effects of adding incompatible software to an existing system

Unfortunately, these factors can often overcome the IT security technologies that companies and individuals use to protect their information. (We discuss security later in the chapter.) A fourth factor identified by the Security Forum is motivation, as described in *A Closer Look 5.2*.

As you have read throughout this book, business success depends on fast and easy access to accurate information—and keeping it protected. For e-commerce to survive, with its potential number and scope of customers, companies must invest in complex and expensive information management, identity management, and security management systems. IT security and internal control of this magnitude require an enterprisewide model, which is discussed next.

IT SECURITY AND INTERNAL CONTROL MODEL

Successful implementation of any 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. It 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 5.4. The



Senior Management Commitment & Support

Security Policies & Training

Security Procedures & Enforcement

Security Tools: Hardware & Software

Figure 5.4 Enterprisewide information security and internal control model.

A Closer Look 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 because it corrupts government and corporate officials and sometimes entire legal systems. It undermines free enterprise by crowding out the private sector, and it threatens the financial stability of countries and the international free flow of capital.

Like money laundering, terrorist financing represents an exploitable vulnerability. In money laundering, transnational organized crime groups deliberately distance themselves from the actual crime, but they are never far from the eventual revenue stream. By contrast, 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-Qaida 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).

model views infosec as a combination of people, processes, and technology. We examine the four steps in this model below. For detailed practices and guidelines for insuring Internet security, see *Online Brief 5.1 Managing Internet Security.*

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 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 will be discussed in detail in Section 5.6.

Step 2: Security Policies and 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. Survey results in *A Closer Look 5.3* illustrate the importance of AUP training and consent, particularly because of increased use of handheld devices.

The key findings from the CompTIA Research Survey released in April 2008 are the following:

- Infosec is seen as a key risk among firms, with 80% of US respondents indicating that it is considered top priority by management. Nearly two-thirds of US firms, more than half of UK and Chinese firms, and two-fifths of Canadian firms have implemented written IT security policies.
- The most widespread threats in the United States stem from spyware, the lack of user awareness, and virus and worm attacks. Canadian organizations indicate riskier browser-based attacks and wireless networking security. Chinese organizations indicate significant threats from spyware, viruses, worms, and browser-based attacks.
- The percentage of their IT budget that companies dedicate to security is growing. In the United States, companies allocated 12% of their IT budget in 2007 for security purposes—up from only 7% in 2005.

A Closer Look 5.3

Mobile Workers and Handheld Devices

CompTIA commissions major research projects on infosec and the workforce. Their 2007 study indentified new threats coming from remote and mobile worker, and the unique set of security challenges that these workers pose to organizations. A majority of the organizations surveyed said handheld devices and wireless networks for data access and transfer have increased security risks.

The increasing pervasiveness of remote access to confidential data and applications by mobile employees and wireless networks creates vulnerabilities. Each remote connection or access point is another potential security vulnerability that must be secured. The survey also revealed a change in priorities from protecting sensitive data from attack by outsiders to addressing internal threats. Nearly 80 percent cited the human factor as the root cause for information security failures. That result is not surprising given that only 32 percent of companies that allow data access by remote or mobile employees have implemented security awareness training programs for these employees.

Sources: Compiled from Venator (2007) and Westervelt (2007).

For Further Exploration: What are some reasons why employees do not follow internal security policies and procedures? How can they be motivated to diligently follow AUPs and security procedures?

Companies spend substantial amounts on prevention because security breaches can be costly if they occur. In the past year, US firms shelled out an average of over $200,000 as a result of security breaches, a third of which was attributed to the loss of employee productivity. Moreover, in the last year in the US, Canada and UK, IT staff members spent over 10% of their time dealing with security breaches, and in China, almost 20% of their time.

Step 3: 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.

FIN HRM MKT

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 cell phone or car would have a 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

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?

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

Step 4: Security Tools: Hardware and Software. The last step in the model is implementation of software and hardware needed to support the policy and enforce secure practices. Keep in mind that security is an ongoing process and not a problem that can be solved with hardware or software tools. Hardware and software security defenses cannot protect against irresponsible business practices. For more information on the reasons for a multilayered security approach, read *Online Brief 5.2 Spyware: A Financial Assault Weapon*. We cover basic security hardware and software later in the chapter.

Review Questions

1. Why are cleanup costs after a single data breach or infosec incident in 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 service pack?
5. What are two causes of the top information problems at organizations?
6. 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 vulnerabilities and threats. Most workers use their PCs and laptops 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 personal computers remains risky because, despite years of policies designed to control them, employees continue to engage in dangerous surfing and communication habits that can 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** play a role in many computer problems, as you have read. Errors can occur in the design of the hardware or information system. They can also occur in the programming, testing, data collection, data entry, authorization, and instructions. Not changing default passwords on a firewall creates a security hole. Human errors contribute to the majority of internal control and infosec problems.
- **Environmental hazards** include earthquakes, severe storms (e.g., hurricanes, blizzards, or sand), 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 recreated.
- **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 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. See *Online Brief 5.3 VoIP Security Alert: Hackers Attack for Cash* for an example. The scope of intentional threats can be against an entire country or economy. Defenses against the possibility of *cyberattacks* by some countries against others are identified in *A Closer Look 5.4*.

Intentional crimes carried out on the Internet are called cybercrimes (also discussed later). **Hacker** is the term often used to describe someone who gains unauthorized access to a computer system. *Black-hat hackers*, also referred to as crackers, are criminals. A **cracker** is a *malicious hacker,* who may represent a serious problem for a corporation.

Hackers and crackers may involve unsuspecting insiders in their crimes. In a strategy called **social engineering,** criminals or corporate spies trick insiders into giving them information or access that they should not have. Social engineering is a collection of tactics used to manipulate people into performing actions or divulging confidential information. 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 *A Closer Look 5.5.* 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.

METHODS OF ATTACK ON COMPUTING FACILITIES

There are many methods of attack, and new ones appear regularly. In this section, we look at some of these methods. Two basic approaches are used in deliberate attacks on computer systems: 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 when someone enters false, fabricated, 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.

Programming attacks are popular with computer 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. Examples are

A Closer Look 5.4

Global IT Security Efforts

Most countries are updating laws and regulations to protect networked information.

- In May 2006, Transport and Communication Minister Christopher Mushowe announced the government of Zimbabwe would pass legislation to curb cybercrime in the country in view of its increasing threat to world economies.
- Zhang Changsheng, Vice President of China Netcom, stated that China Netcom would play an active role in a series of countermeasures, including regulation on SMS and mobile services, registration of mobile phone users' legal names, cleaning up Internet domain names, and elimination of spam.
- In 2006, the U.S. Department of Homeland Security (DHS) launched *Cyber Storm*, the first wide-scale government-led IT security exercise to examine response, coordination, and recovery mechanisms in simulated cyberattacks against critical infrastructures. One of the exercise scenarios simulated a breach against a utility company's computer systems, causing numerous disruptions to the power grid. The exercise was done to show the interconnectivity between computer and physical infrastructures.

A Closer Look 5.5

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, which has since been shut down. 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 were all less than one month old, and consisted of 5,388 unique log files from around the world. The server had been running for three weeks before it was found. Data were 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 were stolen.

Dubbed a *crime server,* it held more than 1.4 gigabytes of business and personal data stolen from computers infected with Trojan horses. While gathering data, it was also 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 him control over the uses of the crimeware and its victims. Since the crime server's stolen data were left without any access restrictions or encryption, the data were freely available for 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).

viruses, worms, and Trojan horses, which are types of malicious code, called **malware.** Programming attacks appear under many names, as shown in *Online Brief 5.3.* 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.

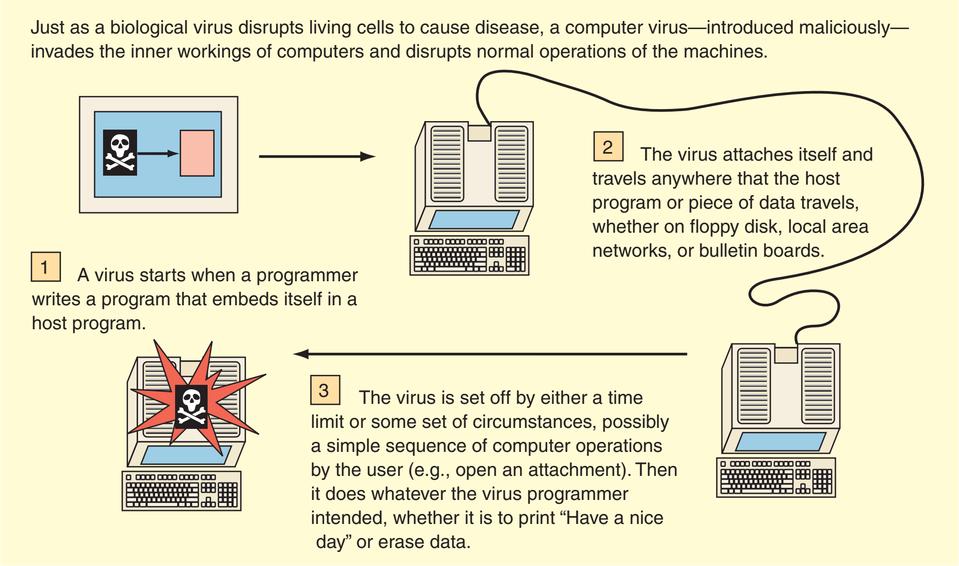
Malware. Malware is any unwanted software that exploits flaws in other software to gain illicit access. In 2007, malware fundamentally changed as criminals used the Internet as the primary attack vector for infecting computers. As more companies defended their e-mail **gateways** against intruders with stronger security mechanisms, cybercriminals shifted their efforts to planting malware on insecure Web sites, waiting for visitors, and then infecting them. A gateway is a network access point that acts as an entrance to other networks.

In the past, virus writers were typically motivated by fame or mischief, but today's attacks are organized attacks designed to steal data and resources from the computers of victims for profit. The scale of their global criminal operations is so extensive that computer security company Sophos (sophos.*com*) discovers a new infected Web page every 14 seconds—24 hours a day, 365 days a year.

Virus. A universal attack method is the **virus,** which is computer code (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 5.5. When the infected software is used, the virus spreads, causing damage to that program and possibly to others.

Worm. 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 horse or RAT. Trojans 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



Just as a biological virus disrupts living cells to cause disease, a computer virus—introduced maliciously—invades the inner workings of computers and disrupts normal operations of the machines.

1 A virus starts when a programmer writes a program that embeds itself in a host program.

2 The virus attaches itself and travels anywhere that the host program or piece of data travels, whether on floppy disk, local area networks, or bulletin boards.

3 The virus is set off by either a time limit or some set of circumstances, possibly a simple sequence of computer operations by the user (e.g., open an attachment). Then it does whatever the virus programmer intended, whether it is to print "Have a nice day" or erase data.

Figure 5.5 How a computer virus can spread.

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 *A Closer Look 5.5* 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 horse attaches itself to a zombie's operating system 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 zombied 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.

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 the most prevalent botnet agent and is embedded inside up to 25 million computers. Storm's combined power has been compared to the processing might of a supercomputer, and Storm-organized attacks are reputed to be 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 email 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:** Perhaps the most ominous botnet threat, and the one that's toughest to counter, is one in which infected computers are rounded up and commanded to overload and cripple a targeted Web site.

The combined power of botnets can scan for and compromise other computers, and then be used for every type of crime and attack against computers, servers, and networks.

MALWARE 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. **Anti-Malware Technology:** 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 IPS have the power and analysis capabilities to detect and block DoS attacks, functioning somewhat like an automated circuit breaker.

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

In the next section, we discuss crime—specifically fraud, which is also known as white-collar crime, and computer 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 and Computer-Mediated Crimes

Crime can be divided into two categories: violent crime and nonviolent crime. Fraud is nonviolent crime. Instead of a gun or knife, fraudsters use deception, confidence, and trickery. Fraudsters carry out their crime by abusing the power of their position or taking advantage of the trust of others. While statistics show that violent crime is down, fraud is at an all-time high and shows no signs of diminishing.

Computer crimes appear frequently and with novel names that quickly become part of our everyday vocabulary. For example, spyware researchers at Webroot Software had uncovered a stash of tens of thousands of stolen identities from 125 countries that they believe were collected by a new variant of a Trojan program the company named Trojan-Phisher-Rebery. Rebery is an example of a banking Trojan, which is programmed to come to life when users visit one of a number of online banking or e-commerce sites. Without strong defenses—including AUP and secure procedures—e-commerce can lose a lot of customers. Next, we discuss the most common and devastating types of fraud and computer crimes.

FRAUD

When a person uses his or her occupation for personal gain through deliberate misuse of the organization's resources or assets, it is called **occupational fraud.** Examples of occupational fraud are listed in Table 5.3.

Internal audits and internal controls (covered later in the chapter) are critical to the prevention and detection of occupation frauds. High-profile examples of occupational fraud committed by senior executives during the early 2000s that led to increased government and SEC regulation, such as SOX, include the following:

- **Adelphia.** A year after the public learned of the $600 million Enron scandal, several chief executive officers of Adelphia, including John Rigas and Tim Rigas, made Enron's fraud look small. The SEC uncovered the misappropriation and theft of tens of billions of dollars by some of Adelphia's chief executives. In addition to the $2.3 billion that was stolen from the company, the fraud caused losses to investors of more than $60 billion.
- **Global Crossing.** Corporate insiders knowingly sold more than $1.5 billion of artificially inflated company stock. In April 2005, the SEC filed a settled action for civil penalties against Global Crossing's former CEO, CFO, and VP of Finance for aiding and abetting the fraud. Each executive agreed to pay a $100,000 civil penalty.
- **Tyco.** In 2003, the SEC charged former CEO Dennis Kozlowski, CFO Swartz, and Chief Corporate Counsel Mark Belnick with many counts of fraud. Kozlowski and Swartz had swindled over $170 million in corporate loans and pocketed $430 million by manipulating the company's stock price. Belnick was indicted for falsifying business records to hide $17 million in loans given to him by Tyco.

INTERNAL FRAUD PREVENTION AND DETECTION

IT has a key role to play in demonstrating good corporate governance and fraud prevention. Regulators look favorably on companies that can demonstrate good corporate governance and best practice operational risk management. Management and

TABLE 5.3 Types of Organizational Fraud

Type of fraud	Financial statement fraud?	Typical characteristics
Operating management corruption	No	Occurs *off the books.* Median loss due to corruption: over 6 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"		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	"Earnings management" in violation of GAAP (Generally Accepted Accounting Principles); see *aicpa.org*

staff of such companies will 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.

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 human resources and finance departments. The data are stored in a data warehouse where they are analyzed to detect anomalous patterns, such as excessive hours worked, deviations in patterns of behavior, copying 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.

ETHICS

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 in addition to the direct cost of the loss. It 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 dumpster digging. 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 that force those notifications. Examples in Table 5.4 illustrate different ways in which identity crimes have occurred.

Furthermore, computer criminals do not need IT skills to steal a laptop (recall the VA employee's home robbery), cell, or PDA, or find one that was left behind. Therefore, unencrypted sensitive data on laptops or handheld devices that leave the office increase the risk.

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 login information	33,000	The U.S. Air Force suffered a security breach in the online system containing information on officers and enlisted airmen, and personal information.
Missing backup	200,000 tape	A timeshare unit of Marriott International Inc. lost a backup tape containing SSNs and other confidential data of employees and timeshare owners and customers.

TOP CYBER SECURITY MENACES

The SANS (SysAdmin, Audit, Networking, and Security) Institute publishes a yearly list of the top 10 cybersecurity threats. The list for 2008 includes new exploitations of browser vulnerabilities; worms with advanced P2P (peer-to-peer) technologies; and insider attacks by rogue employees, consultants or contractors. Twelve cyber security experts worked together to compile the following list of the attacks most likely to cause substantial damage during 2008 (see *sans.org/2008menaces*).

1. Increasingly Sophisticated Web Site Attacks that Exploit Browser Vulnerabilities—Especially on Trusted Web Sites. Web site attacks on browsers are targeting components, such as Flash and QuickTime, that are not automatically patched when the browser is patched. Also, Web site attacks are more sophisticated attacks that can disguise their destructive payloads (the malicious part of the malware). Attackers are putting exploit code on popular, trusted Web sites that visitors believe are secure. Putting hidden attack tools on trusted sites gives attackers a huge advantage.

2. Increasing Sophistication and Effectiveness in Botnets. Storm worm, which was not a worm, began spreading in January 2007 with an e-mail saying, "230 dead as storm batters Europe," and was followed by subsequent variants. Within a week, it accounted for one out of every twelve infections on the Internet, installing **rootkits** (sets of network administration tools to take control of the network) and making each infected system a member of a new type of botnet. Previous botnets used centralized command and control; the Storm worm used peer-to-peer (P2P) networks to launch (control) the attack, so there is no central controller to take down to stop it. New variants and increasing sophistication will keep Storm worm and other even more sophisticated worms as serious threats.

3. Cyber Espionage Efforts by Well-Resourced Organizations Looking to Extract Large Amounts of Data, and Phishing. One of the biggest security stories of 2007 was disclosure of massive penetration of federal agencies and defense contractors and theft of terabytes of data. Economic espionage will increase as nations steal data to gain economic advantage in multinational deals. The attack involves targeted phishing with attachments, using social engineering methods so the victim trusts the attachment.

4. Mobile Phone Threats, Especially against iPhones and VoIP. Mobile phones are general purpose computers so they are targeted by malware. A mobile platform is also a platform for unforeseen security risks. The developer toolkits provide easy access for hackers. Vulnerabilities of VoIP phones and attack tools that exploit those vulnerabilities have been published on the Internet.

5. Insider Attacks. Insiders have a significant head start in attacks that they can launch. Insider-related risk as well as outsider risk has skyrocketed. Organizations need to put into place substantial defenses against this kind of risk, one of the most basic of which is limiting access according to what users need to do their jobs.

6. Advanced Identity Theft from Persistent Bots. A new generation of identity theft is being powered by bots that stay on machines for three to five months collecting passwords, bank account information, surfing history, frequently used email addresses, and more. They will gather enough data for advanced identify theft until criminals have enough data to pass basic security checks.

7. Increasingly Malicious Spyware. Criminals and nations continue to improve the capabilities of their malware. Additionally, some of Storm variants are able to detect investigators' activity and respond with a DoS attack against the investigators, making investigation more difficult. Advanced tools will resist anti-virus, anti-spyware, and anti-rootkit tools to help preserve the attacker's control of a victim machine. In short, malware will become stickier on target machines and more difficult to shut down.

8. Web Application Security Exploits. Large percentages of Web sites have vulnerabilities resulting from programming errors. Adding to the risk exposure are Web 2.0 applications that are vulnerable because user-supplied data (which could have been supplied by hackers or others with malicious intent) cannot be trusted. In 2008, web attacks will increase because of the exposure created by Web 2.0 vulnerabilities and programming errors.

9. Increasingly Sophisticated Social Engineering Including Blending Phishing with VoIP and Event Phishing. Blended approaches will increase the impact of common attacks. For example, the success of phishing is increased by first stealing users' IDs. A second area of blended phishing combines e-mail and VoIP. An inbound e-mail, disguised to look as though it was by a legitimate credit card company, asks recipients to re-authorize their credit cards by calling a 1-800 number. The number leads them via VoIP to an automated system in a foreign country that asks that they key in their credit card information.

10. Supply Chain Attacks Infecting Devices (e.g., thumb drives and GPS) Distributed by Trusted Organizations. Retailers are becoming unwitting distributors of malware. Devices with USB connections and CDs packaged with them sometimes contain malware that infect victims' computers and connect them into botnets. Even more targeted attacks using the same technique are starting to hit conference attendees who are given USB thumb drives and CDs that supposedly contain just the conference papers, but also contain malicious software.

There is a growing tendency for workers to blur their personal and professional lives. For example, they are surfing social networking sites or IMing with friends while at work. And they are accessing corporate networks from hot spots while on vacation. These are very dangerous trends.

Review Questions

1. Define fraud and occupational fraud. Give two examples of each.
2. Explain why data on laptops and computers should be encrypted.
3. What is a rootkit? Explain why hackers use them.
4. Why are Web 2.0 applications vulnerable?
5. Why is spyware expected to grow more malicious?

5.4 IT Security Management Practices

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. Like 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). This objective is to minimize or limit 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,

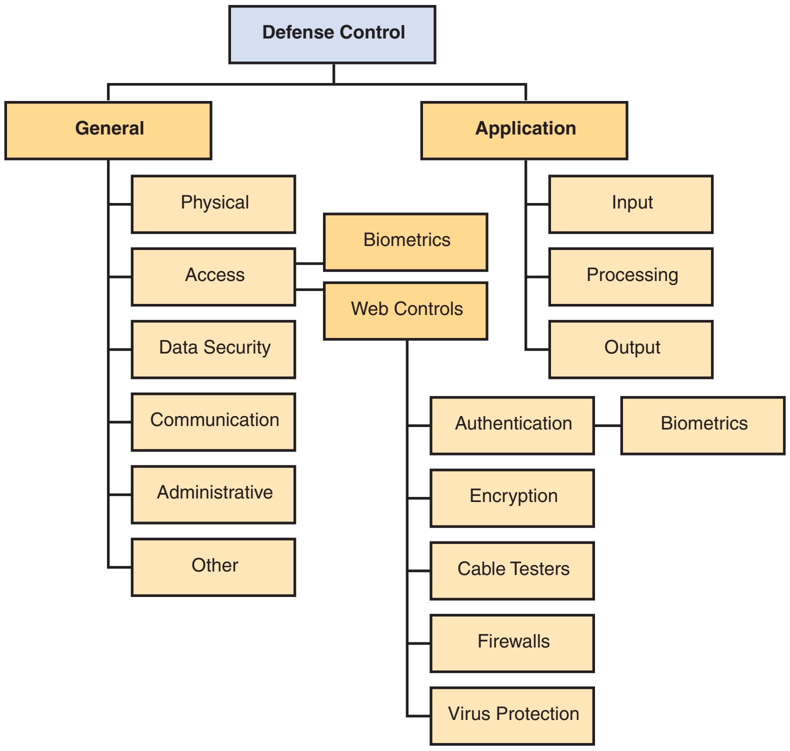


Figure 5.6 Major defense controls.

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 is also going to require 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, data security controls, communication network controls, and administrative 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 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, the site should be 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 Control. 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 claims to be). Authentication methods include

- Something only the user *knows*, such as a password
- Something only the user *has*, for example, a smart card or a token
- Something only the user *is*, 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 prestored profile. The most common biometrics are:

- **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 back-of-the-eye 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.

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

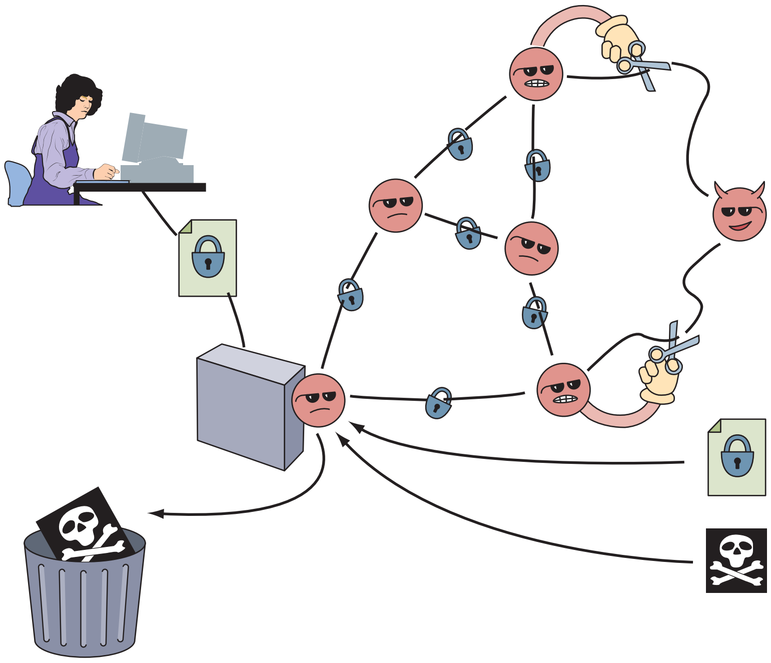


Figure 5.7 Intelligent agents. *(Source: Courtesy of Sandia National Laboratories.)*

Agents in 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.

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 referred to as softbots or knowbots, are highly intelligent 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 perimeter—the network. We discuss the security of wireline and wireless networks and their inherent vulnerabilities.

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 four examples.
5. What is the general meaning of intelligent agents?

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.

Network security measures involve three layers: *perimeter security* (access), *authentication,* and *authorization.* Details of these layers are shown in Figure 5.8. Some commercial products include security measures for all three levels—all in one product, e.g., WebShield from McAfee. Many security methods and products are available to protect the Web. We briefly describe the major ones in the following sections.

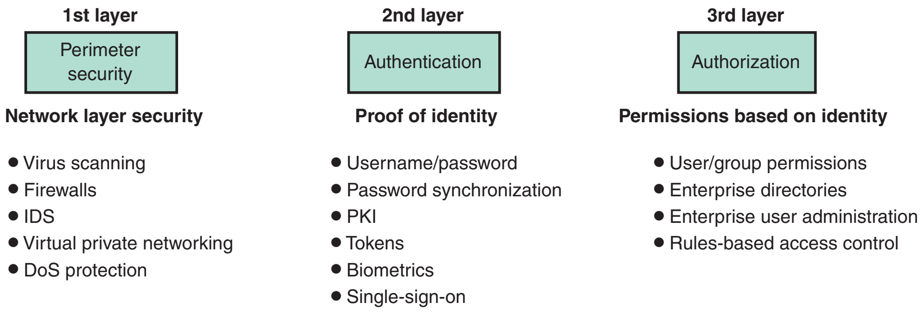


Figure 5.8 Three layers of network security measures.

PERIMETER SECURITY AND FIREWALLS

The major objective of perimeter security is access control, as seen in Figure 5.8. The technologies used to protect against malware (e.g., IDS and IDP) also protect the perimeter. Another technology is firewalls. 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. The firewall follows strict guidelines that either permit or block traffic; therefore, a successful firewall is designed with clear and specific rules about what can pass through. Several firewalls may exist in one information system. Useful as they are, firewalls do not stop viruses that may be lurking in networks. Viruses can pass through the firewalls, especially if they are hidden in an e-mail attachment.

All Internet traffic (i.e., packets) needs to pass through a firewall, but that is rarely the case for IM 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 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 (see Figure 5.8). 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.

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 if 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 (APs or WAPs) behind a firewall and other security protections can be a backdoor into a network. Sensitive data that are not encrypted or that are encrypted with a weak cryptographic technique used for wireless, such as **wired equivalent privacy (WEP),** and that are transmitted between two wireless devices may be intercepted and disclosed. Wireless devices are susceptible to DoS attacks because intruders may be able to gain connectivity to network management controls and then disable or disrupt operations. Wireless packet analyzers, such as AirSnort and WEPcrack, are readily available tools putting wireless networks at great risk.

Unauthorized wireless APs could be deployed by malicious users—tricking legitimate users to connect to those rogue access points. Malicious users then gain access to sensitive information stored on client machines, including logins, passwords, customer information, and intellectual property.

Through war driving, malicious users can connect to an unsecured wireless AP and gain access to the network. See *A Closer Look 5.6* for details on war driving. Data can be extracted without detection from improperly configured devices. *Online Brief 5.3* also describes wireless and VoIP security. A schematic view of all major defense mechanisms, which protect against attackers of all types, is shown in Figure 5.9.

With an understanding of the vulnerabilities, risk exposure, and types of crimes committed with or against IT resources, we examine issues of great importance to executive management and the entire enterprise—internal control and compliance management.

Review Questions

1. What are network access control (NAC) products?
2. Define authentication, and give three examples of authentication methods.
3. Define authorization.
4. What is a firewall? What can it *not* protect against?
5. Define war driving and a resulting risk.

A Closer Look 5.6

War Driving

A number of people have also made a hobby or sport out of war driving. **War driving** is the act of locating wireless local area networks while driving around a city or elsewhere (see *wardriving.com*). To war drive, you need a vehicle, a computer or PDA, a wireless card, and some kind of an antenna that can be mounted on top of or positioned inside the car.

Because a WLAN (wireless local area network) may have a range that extends beyond the building in which it is located, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to important data and other resources.

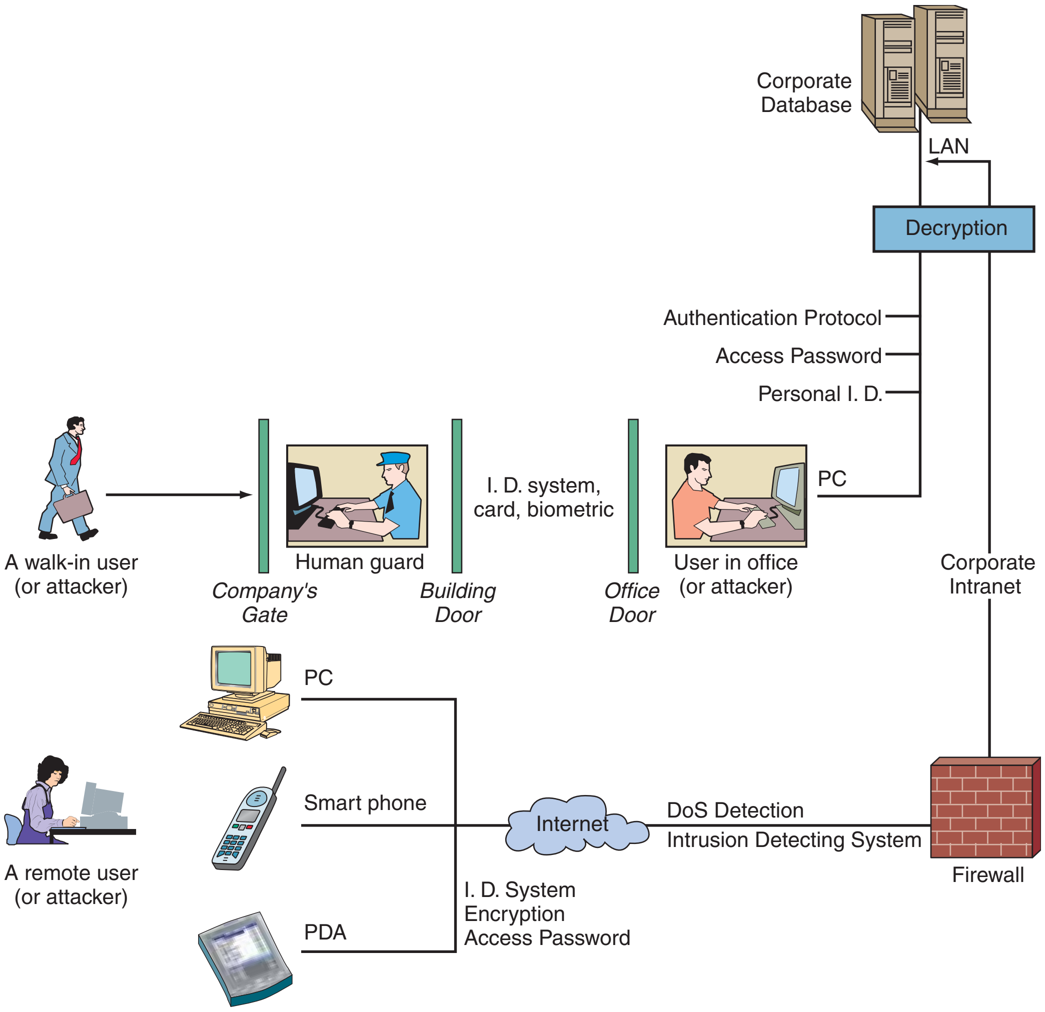


Figure 5.9 Where the defense mechanisms are located.

5.6 Internal Control and Compliance Management

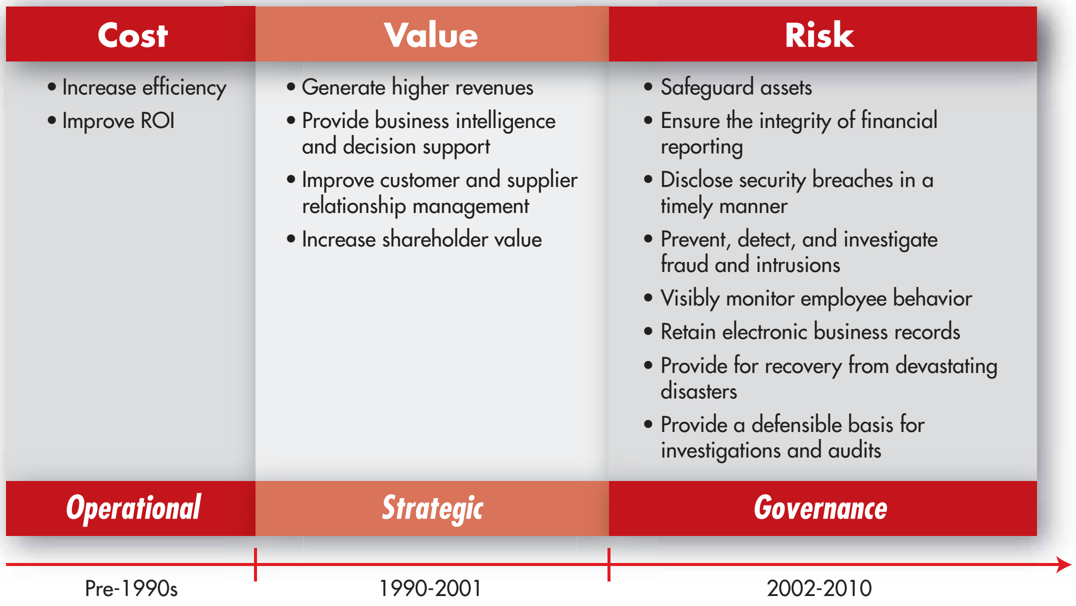
The **internal control environment** is the work atmosphere that a company sets for its employees. *Internal control (IC)* is a process designed to achieve: (1) reliability of financial reporting, (2) operational efficiency, (3) compliance with laws, (4) regulations and policies, and (5) safeguarding of assets. Figure 5.10 illustrates how the role of IT in internal control has changed.

INTERNAL CONTROLS REQUIRED TO BE SOX COMPLIANT

SOX is an antifraud law. It forces better 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



Cost	Value	Risk
• Increase efficiency • Improve ROI	• Generate higher revenues • Provide business intelligence and decision support • Improve customer and supplier relationship management • Increase shareholder value	• Safeguard assets • Ensure the integrity of financial reporting • Disclose security breaches in a timely manner • Prevent, detect, and investigate fraud and intrusions • Visibly monitor employee behavior • Retain electronic business records • Provide for recovery from devastating disasters • Provide a defensible basis for investigations and audits
Operational	*Strategic*	*Governance*
Pre-1990s	1990-2001	2002-2010

Figure 5.10 Increasing role of IT in internal control.

"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."

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 the company can find out everything that every employee does and use that evidence to prosecute that person to the fullest extent, then the feeling that "I can get away with it" drops drastically.

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 go out of their way to work overtime
A large drop in profits
A major increase in business with one particular customer
Customers complaining about double billing
Repeated duplicate payments
Employees with the same address or telephone number as a vendor

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

WORLDWIDE ANTI-FRAUD REGULATORS

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 has been fined for weaknesses in antifraud systems by the FSA, which warned that it is "raising its game" against firms with lax controls.

There is also the Basel II Accord (named after Basel, Switzerland; also called the *Basel II Capital Accord*) that imposes rigorous antifraud requirements for banks. This Accord aims to promote enhanced risk-management practices among large, international banking organizations. For current issues on Basel II, see The Federal Reserve Bank at *federalreserve.gov/GeneralInfo/basel2/*. The Basel II Capital Accord provides guidance for managing operational risk and internal fraud. It recommends that any internal risk measurement system be consistent with the following seven types of potential losses:

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety
4. Clients, products, and business practices
5. Damage to physical assets
6. Business disruption and systems failures
7. Execution, delivery, and process management

Managing risk has become the single most important issue for the 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. What is the role of IT in internal control? (see Figure 5.10)
3. How does SOX Section 302 deter fraud?
4. List three symptoms or red flags of fraud that can be detected by internal controls.
5. What does the Basel II Accord recommend?

5.7 Business Continuity and Disaster Recovery Planning

Disasters may occur without warning. The best defense is to be prepared. Therefore, 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. Therefore, it is difficult for many organizations to obtain insurance for their computers and information systems

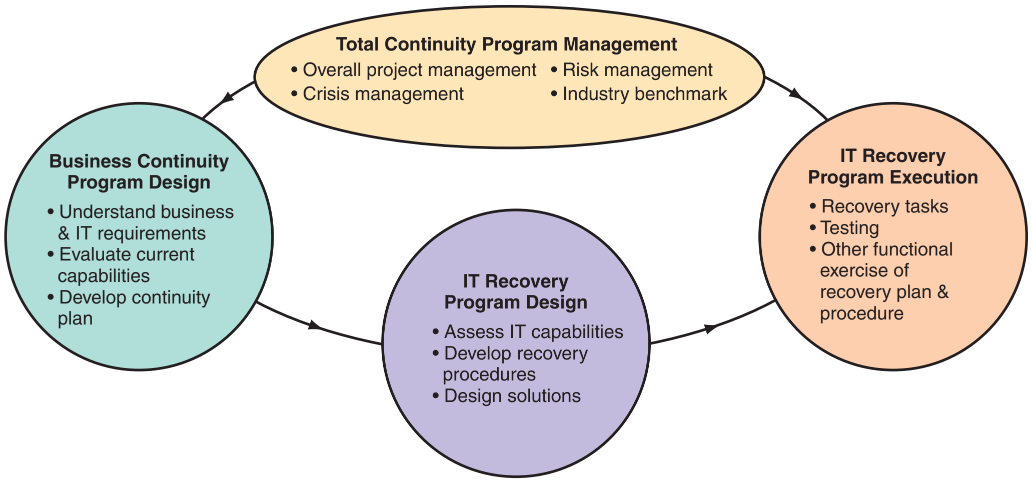

Total Continuity Program Management
• Overall project management
• Crisis management
• Risk management
• Industry benchmark
Business Continuity Program Design
• Understand business & IT requirements
• Evaluate current capabilities
• Develop continuity plan
IT Recovery Program Design
• Assess IT capabilities
• Develop recovery procedures
• Design solutions
IT Recovery Program Execution
• Recovery tasks
• Testing
• Other functional exercise of recovery plan & procedure

Figure 5.11 Business continuity services managed by IBM. *(Courtesy of IBM)*

without showing a satisfactory disaster prevention and recovery plan. The comprehensiveness of a business recovery plan is shown in Figure 5.11.

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.
- 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. See *IT at Work 5.2* for a discussion of the importance of business continuity and the ability to recover from a disaster.

Disaster Avoidance. **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.

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.

IT at Work 5.2

Business Continuity and Disaster Recovery

Ninety-three percent of companies that suffer a significant data loss die within five years, according to Freeman Mendel, the chair of the FBI's 2006 Infragard National Conference. 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.

Globally, regulators are increasingly paying closer attention to business continuity and recovery times, which are now measured in hours rather than days. The Australian Prudential Regulation Authority (APRA) released its prudential standard on business continuity in April 2005. APRA gave Australian firms only 12 months to fix their compliance gaps.

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

For Further Exploration: 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?

5.8 Auditing and Risk Management

Implementing controls in an organization can be a very complicated task, particularly in large, decentralized companies where administrative controls may be difficult to enforce. Of the many issues involved in implementing controls, three are described here: auditing information systems, risk analysis, and IT security trends, including use of advanced intelligent systems.

Controls are established to ensure that information systems work properly. Controls can be installed in the original system, or they can be added once a system is in operation. Installing controls is necessary but not sufficient. It is also necessary to answer questions such as the following: Are controls installed as intended? Are they effective? Are they working reliably? Did any breach of security occur? If so, what actions are required to prevent recurrence? These questions need to be answered by independent and unbiased observers. Such observers perform the information system *auditing* task.

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 as 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 EC is also more complex since, in addition to the Web site, one needs to audit order taking, order fulfillment, and all support systems.

RISK-MANAGEMENT AND 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:

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

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 rights. A Gartner Group study showed that even after the terrorist attacks of 9/11/2001, only 26 percent of Americans approved a national ID database. Using biometrics is considered by many 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, or 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 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 (see *epolicyinstitute.com*).

Review Questions

1. What are auditing information systems?
2. Why should Web sites be audited?
3. How can expected loss be calculated?
4. List two ethical issues associated with security programs.
5. How have wireless technologies and a mobile workforce influenced the scope of employment?
6. Define the doctrine of duty of care.

5.9 Managerial Issues

1. What is the business value of IT security and internal control? IT security risks are business risks. IT security is so integral to business objectives that it cannot be treated as a stand-alone function. Information security has evolved into a core business issue with legal obligations.

2. Why are there legal obligations? The legal issues surrounding information security are rooted in the fact that virtually all of a company's daily transactions and confidential records are created, used, communicated, and stored in electronic form and must be protected.

3. How important is IT security to management? Management's obligation to insure data security has increased significantly. The financial damages and disruption caused by hackers, phishers, spammers, identity thieves, malware, and terrorists worldwide are tremendous.

4. IT security and internal control must be implemented top-down. Effective enterprisewide IT security begins with senior management commitment and support. The power of senior managers is needed to enforce secure and ethical security and privacy practices.

5. Acceptable use policies (AUPs) and security awareness training are important for any organization. The number one threat to IT security since 2002 has been human error. IT security depends on people as well as processes and technology.

6. Digital assets are relied upon for competitive advantage. At a strategic level, the totality of a company's data resources is nearly irreplaceable. BI, ERP, CRM, and e-commerce business operations depend on the integrity, availability, and authorized use of IT resources.

7. What does risk management involve? Risk management includes securing corporate systems, networks, and data; ensuring availability of systems and services; planning for disaster recovery and business continuity; complying with government regulations and license agreements; and protecting the organization against malware, spyware, and profit-motivated hacking.

8. What are the impacts of IT security breaches? Privacy breaches and security incidents lead to fines and customer attrition. IT security failures have a direct impact on business performance because they can no longer be hidden.

9. Federal and state regulations. Stringent federal and state regulations are having a major impact on data security practices. Record-setting fines are being used to compel management to invest in all reasonable security defenses.

10. Internal control. If internal controls can be ignored, there is no control. If the company shows its employees that the company can find out everything that every employee does and use that evidence to prosecute that person to the fullest extent, then the feeling that "I can get away with it" drops drastically.

How *IT* Benefits You

Pressure to meet compliance, security, and risk management responsibilities is felt by every business department. Defenses against formidable external and internal threats, business continuity, and quick recovery from control and policy failures are demanded by customers, trading partners, investors, regulators, professional ethics boards, and various laws.

For the Accounting Major

The information security requirements for public companies, their accountants, and auditors have changed significantly. Accountants are being held professionally responsible for reducing risk, assuring compliance, eliminating fraud, and increasing the transparency of transactions according to GAAP (Generally Accepted Accounting Principles). The SEC and PCAOB (Public Company Accounting Oversight Board), among other regulatory agencies, demand information security, fraud prevention and detection, and internal controls over financial reporting. One of the hottest accounting careers is forensic accounting.

For the Finance Major

As IT security becomes ever more critical to the success of any organization, it is no longer just the concern of the CTO or CIO. With global regulatory requirements and Sarbanes-Oxley §302, responsibility for information security lies with the CEO and CFO. As a result, all aspects of the audit, including security of information and IT systems, are a key concern for the finance function.

At the same time, CFOs and treasurers are increasingly involved in IT investment decision making. They are realizing that a security breach of any kind can have catastrophic financial effects on a company. Just as it is important to have a good insurance policy in place to protect against unforeseen business circumstances, so, too, is it important to have good security protocols in effect to protect against unforeseen attacks.

For the Human Resources Management Major

The HR function is responsible for two key legal obligations: (1) the duty to provide reasonable security for their corporate data and information systems, and (2) the duty to disclose security breaches to those who may be affected adversely by them. HR departments have clear obligations to secure confidential employee data and provide a nonhostile work environment. Getting explicit consent from all employees verifying that they understand the acceptable use policy is a critical defense against charges of harassment, discrimination, and wrongful termination.

For the IS Major

All application development, network deployment, and introduction of new IT have to be guided by IT security considerations. Some of the technologies the IS department must understand are spam filtering, VoIP, WEP, server access controls, intrusion detection, encryption, password management, authentication, and biometrics. The IS department must customize the risk exposure security model to help the company identify security risks and prepare responses to incidents or disasters.

Senior executives look to the ISD for help in meeting its SOX mandates, particularly in detecting "significant deficiencies" or "material weaknesses" in internal controls and remediating them. Other departments look to the ISD to help them meet their security responsibilities.

For the Marketing Major

Customers expect their data to be safe. Profit-motivated hackers want those data. Marketers need to weigh the risk exposure of their operations. Failure to protect corporate and customer data is likely to bring on significant public relations problems and enrage customers. CRM operations and tracking customers' online buying habits can expose data to misuse (if not encrypted) or result in privacy violations. Marketers need to insure customer data security and privacy, which can be used to attract and retain customers.

For the Production/Operations Management Major

Every process in a company's operations—inventory purchasing, receiving, quality control, production, and shipping—can be disrupted by an IT security failure or the failure of a trading partner. Basically, any weak link in supply chain management or enterprise resource management systems puts everyone at risk. Companies are held liable for IT security failures that impact other companies.

Key Terms

Acceptable use policy (AUP)	*161*
Access control	*173*
Administrative controls	*173*
Adware	*166*
Application controls	*172*
Audit	*181*
Biometric control	*173*
Business continuity plan	*179*
Business impact analysis (BIA)	*162*
Computer systems failures	*163*
Corporate governance	*154*
Cracker	*164*
Crime server	*164*
Data tampering	*164*
Denial of service (DoS) attacks	*165*
Disaster avoidance	*180*
DoS Attacks	*166*
Environmental hazards	*163*
Gateways	*165*
General controls	*172*
Hacker	*164*
Human errors	*163*
Intelligent agents	*174*
Internal control	*161*
Internal control environment	*177*
Internal threats	*155*
IT security	*155*

Malware *165*
Network port *165*
Occupational fraud *168*
Operational risk *155*
Payment Card Industry Data Security Standard (PCI DSS) *159*
Phishing *166*
Physical Controls *172*
Programming attacks *164*
Remote administration Trojans (RATs) *166*
Retinal scan *173*
Rootkits *170*
Service packs *158*
Signature *173*
Social engineering *164*
Spam *166*
Spyware *166*
Thumbprint or fingerprint *173*
Time-to-exploitation *158*
Two-factor authentication *175*
Virus *165*
Voice scan *173*
War driving *176*
Wired equivalent privacy (WEP) *176*
Worm *165*

Chapter Highlights

(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 antifraud 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 they underestimate 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 are 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.

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

8 A large range of IT security tools, including intelligent agents and antifraud measures, help defend against counterterrorist activities.

Virtual Company Assignment

Managing Information Resources and Security at The Wireless Café

Go to The Wireless Café's link on the Student Web Site. There you will be asked to analyze security vulnerabilities of the restaurant's information resources.

Instructions for accessing The Wireless Café Web Site on the Student Web Site:

1. Go to wiley.com/college/turban.
2. Select *Turban/Volonino's Information Technology for Management*, Seventh Edition.
3. Click on Student Resources site, in the toolbar on the left.
4. Click on the link for Virtual Company Web Site.
5. Click on Wireless Café.

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. Describe how IS auditing works and how it is related to traditional accounting and financial auditing.
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. Some people have recently suggested using viruses and similar programs in wars between countries. What is the logic of such a proposal? How could it be implemented?
11. Why is cybercrime expanding rapidly? Discuss some possible solutions.
12. Discuss why the Sarbanes-Oxley Act focuses on internal control. How does that focus influence infosec?
13. 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 security measures that a company implements 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. Read the "Fact Sheet 24(e): Is Your Financial Information Safe?" (at *privacyrights.org/fs/fs24e-FinInfo.htm*) provided by the Privacy Rights Clearinghouse.
   a. Describe the federal Gramm-Leach-Bliley Act (GLB). What does it require of financial institutions?
   b. What must companies do to protect financial information?
4. 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.
5. 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.
6. 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.
7. Should an employer notify employees that their usage of computers is being monitored? Why or why not?
8. Twenty-five thousand messages arrive at an organization each year. Currently there are no firewalls. On the average there are 1.2 successful hackings each year. Each successful hacking 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 3 years. The chance that an intruder will break through the firewall is 0.0002. 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 3 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?
4. Read *In the Matter of BJ's Wholesale Club, Inc.,* Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005 at *ftc.gov/opa/2005/06/bjswholesale.htm.* Describe the security breach at BJ's Wholesale Club. What was the reason for this agreement? Using the enterprisewide IT security and internal control model in Figure 5.4, identify some of the causes of the security breach and how BJ's can better defend itself against hackers and legal liability.

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 their mission is and report on what you think about their 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 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. You have installed a DSL line in your home and you need a firewall. Enter *securitydogs.com, macafee.com,* or *symantec.com*. Find three possible products. Which one do you like best? Why?
13. Access a good search engine (e.g., *google.com* or *findarticles.com*). Find recent articles on disaster planning. Prepare a short report on recent developments in disaster recovery planning.
14. The use of smart cards for electronic storage of user identification, user authentication, changing passwords, and so forth is on the rise. Surf the Internet and report on recent developments.
15. 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?

Minicase

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 until 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 audits, or forced vacation times, 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 ten 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 their 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. By 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), and Yomiuri (2006).

Questions for Minicase

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. Create a table consisting of five columns. In the columns list (1) the company names, (2) the period over which the restatement was made, (3) the incident or regulatory agency that prompted or required the restatement, (4) the impact of earnings, and (5) the stock price at the start of the period of restatement and the stock price soon after the announcement of the restatement.
4. From your Internet search, select four companies that had announced within the past three years that they were restating their earnings, and fill in the first four columns.
5. Use a financial Web site, such as *finance.yahoo.com,* to find the stock prices for the fifth column.
6. What impact did the restatement have on each of the four companies?
7. What internal controls might have prevented or detected the fraud?

Problem-Solving Activity

Estimating Investment in Anti-Spam 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 5.12, 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 anti-spamware. 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 5.12 Model for estimating cost of spam.

Online Resources

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

Online Briefs for Chapter 5 are available at wiley.com/college/turban:

5.1 Managing Internet Security

5.2 Spyware: A Financial Assault Weapon

5.3 Wireless and VoIP Secrity

Online Minicases for Chapter 5 are available at wiley.com/college/turban:

5.1 UBS PaineWebber Debilitated by Malicious Code

5.2 Computer Network Intrusion Affects Millions of Hannaford Shoppers

References

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

CompTIA, *comptia.org* (accessed June 2008).

Computer Economics, *computereconomics.com* (accessed June 2008).

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *coso.org/key.htm* (accessed June 2008).

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

ePolicy Institute, *epolicyinstitute.com* (accessed June 2008).

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

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

Gross, G., "ChoicePoint's Error Sparks Talk of ID Theft Law," *IDG News Service,* February 23, 2005, *pcworld.com/news/article/0,aid, 119790,00.asp* (accessed 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* (accessed June 2008).

Information Security Forum, *securityforum.org* (accessed June 2008).

ISACA, *isaca.org* (accessed June 2008).

IT Governance Institute, *itgi.org* (accessed June 2008).

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

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* (accessed June 2008).

Mimoso, M. S., "Cleaning Up After a Data Attack: CardSystems' Joe Christensen," *Information Security,* April 14, 2006, *searchsecurity. techtarget.com/originalContent/0,289142,sid14_gci1180411,00.html* (accessed June 2008).

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* (accessed June 2008).

Reuters UK, "BNP Paribas Fined for UK Anti-Fraud Failings," May 10, 2007, *uk.reuters.com/article/UK_SMALLCAPSRPT/idUKWLA850120070510* (accessed June 2008).

SANS, Top Ten Cyber Security Menaces for 2008, *sans.org/2008menaces* (accessed June 2008).

Scalet, S. D., "The Five Most Shocking Things About the ChoicePoint Debacle," *CSO,* May 1, 2005.

Sophos, *sophos.com* (accessed June 2008).

Spangler, T., "What You Can Learn from the VA's Snafu," *Baseline,* May 24, 2006, *baselinemag.com/article2/0,1540,1966952,00.asp* (accessed June 2008).

Symantec, *symantec.com* (accessed June 2008).

Taylor, C., "NEC Employees Behind $18M Fraud Scheme," *EDN*, May, 29, 2007a, *dn.com/article/CA6447014.html* (accessed June 2008).

Taylor, C., "NEC Stock Faces Nasdaq Delisting," *EDN*, September 21, 2007b, *edn.com/index.asp?layout=article&articleid=CA6480624* (accessed June 2008).

U.S. Department of State, *state.gov* (accessed June 2008).

Venator, J., "The State of Information Security," *IT Security Journal*, November 27, 2007, *itsecurityjournal.com/index.php/Latest/The-State-of-Information-Security.html* (accessed June 2008).

Westervelt, R., "Employee Error Fuels Data Security Breaches, Survey Finds," *Searchfinancialsecurity.com,* September 24, 2007, *searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1294559,00.html* (accessed June 2008).

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

Yomiuri, "NEC Eyes Charges Over Fake Deals," *The Daily Yomiuri,* March 23, 2006.

Part II Case

Cisco Systems in the Business of Helping Customers Transform Their Businesses

Cisco Systems, Inc. (*cisco.com*) (Nasdaq: CSCO) is a Fortune 500 company, ranking 71 in 2008, that routes data packets and routs its competitors with equal efficiency. Its 2007 net profits were $7.33 billion, with worldwide sales revenues from all product lines totaling almost $35 billion, as shown in Table PII.1. Cisco's Internet protocol (IP) systems remain the backbone of networks used in businesses, home communication, education, and government—that is, anything connected to the Internet. Its IP products are found in most businesses worldwide.

Cisco maintains its market dominance by its skill at identifying business needs far in advance, and then following through by implementing forward-looking business solutions. The company positions itself through numerous acquisitions and collaboration (even with rival Microsoft) to help its customers transform their businesses with Cisco's products and services.

Cisco also helps companies reduce their environmental footprint because consumers and investors are looking more closely at how companies respond to environmental issues. Their keyword phrase is corporate social responsibility (CSR), a term that covers how companies act charitably and responsibly toward employees, the environment, and the developing world. Increasingly, companies are issuing CSR reports along with their annual reports to demonstrate their social commitments. General Electric, British Telecom, Accenture, Exxon, Cisco, and others all do this on a regular basis.

Cisco's Target Customers

Cisco dominates the market for IP-based networking equipment with routers and switches used to direct data, voice, and video traffic. Other products include remote access servers, IP telephony equipment, optical networking components, Internet conferencing systems, set-top boxes, and network service and security systems. Cisco offers products designed for large enterprises and telecommunications service providers, as well as products for small and medium businesses (SMBs). Company growth and expansion of its product lines have been achieved via acquisition of other companies and their products. Acquisitions during 2007 and 2008 are listed in Table PII.2. Comparable numbers of acquisitions had occurred in prior years, too. Cisco also markets products designed for small businesses and consumers through its Linksys division.

The global company, which has regional headquarters in San Jose, Singapore, and Amsterdam, is named after the city of San Francisco.

Company History

Cisco Systems was founded by Stanford University computer science engineers, Len Bosack and Sandra Lerner, and three colleagues in 1984. While working at Stanford, Len, Sandra, and others made major design enhancements to one of the essential Internet technologies, the router. Their multi-protocol router enabled two networks to communicate and share data. These *blue boxes,* as the routers were called, eventually would connect innumerable computers to the Internet. Cisco sold its first network router in 1986. The owners applied for venture capital to start a business marketing the blue boxes, which would become part of infrastructure of data networks and the Internet. But in 1986, that Internet concept had not been proven, making it difficult for them to raise venture capital. After 77 unsuccessful proposals (rejections) to venture capitalists, the group finally raised $2.5 million in venture capital from Sequoia Capital in 1987. The owners continued to develop, and then later to acquire, innovative technologies to support networking.

TABLE PII.1 Cisco Systems, Inc. 2007 Sales by Region and Product Line

	2007 Sales	
Regions	**Sales Revenues (in billions)**	**Percent of Total Sales**
U.S. and Canada	$ 19.29	55%
Europe	$ 7.33	21%
Asia/Pacific Japan	$ 1.29	4%
Other countries	$ 3.55	10%
Emerging markets	$ 3.44	10%
Total	**$ 34.92**	**100%**
Products	**Sales Revenues (in billions)**	**Percent of Total Sales**
Switches	$ 12.47	36%
Advanced technologies	$ 8.07	23%
Routers	$ 6.92	20%
Other	$ 1.99	6%
Services	$ 5.46	15%
Total	**$ 34.92**	**100%**

TABLE PII.2 Cisco Systems' Acquisitions in 2007 and 2008

Acquired Company (and acquisition date)	Products and Capabilities Acquired
DiviTech (June 2008)	digital video networking software
Nuova Systems (April 2008)	data center switches
Securent (November 2007)	security software
Navini Networks (December 2007)	WiMax equipment
Latigent (October 2007)	Web-based business intelligence software for call centers
Cognio (October 2007)	wireless spectrum analysis
BroadWare Technologies (June 2007)	video networking and storage systems
IronPort Systems (June 2007)	Web messaging and email security software
WebEx Communications (May 2007)	Web conferencing systems
Spans Logic (April 2007)	networking semiconductor design
NeoPath Networks (April 2007)	file storage management systems
Utah Street Networks (March 2007)	social networking communities
Reactivity (March 2007)	XML gateways
Five Across (March 2007)	social networking software
Tivella (January 2007)	digital signage software and systems

Also in 1987, Cisco developed the Interior Gateway Routing Protocol, which revolutionized communications between computers by allowing for routing within an autonomous system. By 1989, the company's sales revenues hit $27 million with only three products on the market and 100 employees. With the rise of the World Wide Web, Cisco's web communication products were in very high demand. The company went public on the Nasdaq in 1990, and due to management clashes, owners Len and Sandra sold their stock for about $200 million, giving most to favorite causes, including animal charities and a Harvard professor looking for extraterrestrials. In 1995, John Chambers became chairman and CEO of Cisco Systems, Inc., and remains so as of 2008.

In 1998, Cisco made headlines by becoming the first company in history to reach a market capitalization of $100 billion in only 14 years. But soon afterward, the economic downturn and slump in the telecommunications and technology market were a big hit to Cisco. Its sales revenue dropped for the first time in its history, forcing the company to write off $2.5 billion worth of inventory.

Cisco's Market Breadth Growth Strategy

Cisco has used acquisitions—more than 120 of them since 1993—to broaden its product lines and secure engineering talent in the highly competitive networking sector. Cisco remains committed to investments that insure the dominance of its core lines of switches and routers, which account for 60% of sales, while at the same time moving into new markets through acquisitions. (The diversity of Cisco's acquisitions during 2007 and 2008 are evident in Table PII.2.)

A significant acquisition was WebEx Communications, a leading provider of Internet conferencing systems, for $3.2 billion in 2007. The 2006 acquisition of cable set-top box leader Scientific Atlanta for $6.9 billion was the second largest purchase in its history. Cisco had paid $7 billion for optical networking equipment maker Cerent in 1999. Cisco based its strategy on what it foresaw as the critical importance of technology convergence for data, voice, and television networks. Its acquisition of Scientific Atlanta made it one of the leading providers of the set-top boxes that cable service providers use to deliver advanced features, for example, movies-on-demand. It also put Cisco into a fierce competitive battle with Motorola in the set-top box market.

Key Competitors

Market expansion put Cisco into competition with other megacorporations as well as smart, well-financed upstarts across all of its market segments. Its three top competitors are:

1. **Alcatel–Lucent.** France's Alcatel acquired U.S. rival Lucent Technologies for $11.6 billion in late 2006, forming the new Alcatel–Lucent. The company, with 2007 sales revenues of $26.2 billion, is a leading global supplier of high-tech equipment for telecommunications networks. Specifically, it provides network switching and transmission systems for wireline and wireless networks primarily for telecom carriers, other businesses, and government agencies. Alcatel–Lucent is made up of five business units: wireline, wireless, convergence, enterprise, and services. Alcatel–Lucent's key customers include Verizon, AT&T, BellSouth, and China Telecom.
2. **Juniper Networks.** Juniper Networks has managed to grow in a market dominated by Cisco, with 2007 sales revenues of $2.83 billion. The company designs and sells network infrastructure for private and public access networks. Customers use its products to securely deploy

and manage services and applications across IP networks. The company's product portfolio includes routers, network traffic management software, virtual private network (VPN) and firewall devices, data center and wide area network (WAN) acceleration tools, intrusion detection and prevention (IDP) systems, and support services. Juniper sells directly and through resellers to network service providers, enterprises, government agencies, and schools. Juniper has traditionally catered to Internet and telecommunications service providers, but the company continues to expand its offerings for the enterprise market.

3. **Nortel Networks Corp**. One of the top global makers of telecom equipment in North America, Toronto-based Nortel makes core network switching, enterprise network equipment, wireless, and optical systems for customers worldwide. Despite its 2007 sales revenues of Cdn$10.87 billion, it had a negative net income of almost a billion dollars. In early 2005, Nortel belatedly released its 2003 financial statements following a massive accounting investigation that uncovered billions in fraudulently overstated revenues for the years 1999 and 2000. In early 2006, Nortel agreed to pay $2.5 billion to settle class-action lawsuits that alleged securities laws violations.

Clearly, these are three fierce competitors that Cisco needs to outperform on a daily basis through market intelligence and smart acquisitions. Cisco needs to make strategic decisions so that they are ready when the demand for new products and services arises. For example, the company expanded from a product line limited to hardware by making software investments in 2007, including the acquisition of network and e-mail security applications developer IronPort Systems for $830 million, and wireless spectrum analysis specialist Cognio.

In another competitive move, Cisco entered the social networking sector by acquiring software platform developer Five Across, and assets of Utah Street Networks, the operator of the *Tribe.net* online communities. Cisco acquired WiMax equipment maker Navini Networks for about $330 million in 2007.

Cisco has invested heavily to build its international presence. From 2005 through 2008, the company spent more than $1 billion to expand its operations in India. Late in 2007, it unveiled a $16 billion expansion plan for China, including investments in manufacturing, education programs, and venture capital.

Selling Business Solutions—Not Point Solutions

Much of Cisco's recent success is due to its focus on selling business solutions instead of point products. Businesses are increasingly interested in innovative products that they can count on to integrate and work with other network and IT products. Plus, customers want one company to call upon for help when those devices do not work as promised.

Cisco is focused on developing (or acquiring) its ability to deliver advanced multimedia solutions, applications, and managed services—all of which are based on the network infrastructure. The following strategic initiatives illustrate Cisco's responsiveness and adaptability to the changing markets of its business customers. Those customers want better data management solutions (Chapter 3) and secure high-speed networks that support collaboration and presence and business continuity (Chapters 4 and 5).

Managed Services 3.0—The Market Opportunity Solution Providers Cannot Ignore

In 2008, Cisco launched a massive new Managed Services 3.0 initiative, dubbed *Services 3.0.* Services 3.0 are managed services that vendors (Cisco's customers) can sell to their own customers. Services 3.0 helps vendors, such as telecom carriers, value-added resellers (VARs), and system integrators, to improve their network availability, performance, and data center processes. Managed Services 3.0 give all types of service providers (Internet service providers or application service providers, referred to collectively as xSPs) the ability to take over the management of their customers' IT networks. The benefits to xSPs are the competitive advantages from being able to provide managed services and stronger strategic relationships with customers.

Rather than only supplying bandwidth, xSPs can support their customers' business technology alignment needs, and thereby gain a competitive advantage. Services 3.0 enable vendors to respond to their customers' growing IT and network utilization patterns and future requirements.

Cisco Collaborates with Microsoft to Provide Interoperability

In August 2007, the CEOs of Microsoft and Cisco, Steve Ballmer and John Chambers, together presented a press conference to show the collaborative efforts between the two companies. The discussions were largely focused on informing potential customers and investors of their new collaborative strategy, which is to support the transition to voice, video, and data over the Internet. The companies are designing and building next-generation networks to deliver communications and services over the Internet and to support the transition to Web 2.0 using equipment and software from multiple vendors. This move is significant because Cisco and Microsoft are recognizing that customers need multi-vendor solutions with guaranteed interoperability.

The phrase "Web 2.0" represents the change from the Internet as a "network of networks" with hardwired applications at the end points (e.g., Web sites stored on servers and viewed through browsers, or stand-alone applications on users' computers) to one where networked applications can flexibly use data transported over the Internet in standardized formats.

The network is a platform that connects applications, devices, and ultimately the people using those applications to enable simple manipulation of services, content creation, and input from users. This, together with the move toward delivering triple-play services of voice, video, and data, defines the objectives of closer collaboration between Cisco, a major infrastructure vendor, and Microsoft, the software giant. The two companies have worked together from 1998 to 2008, but have increasingly found that customer requirements have dictated a closer working relationship as next-generation networks are deployed to handle voice, video, and data over a single IP architecture.

While they will collaborate to ensure interoperability and maximize their revenue opportunities, Microsoft and Cisco remain fierce competitors in other markets.

There are seven areas (which were discussed in Chapters 3 through 5) of collaboration between the two companies that are viewed as key areas of development:

1. **IT Architecture:** The companies are optimizing how Windows Vista uses the IP network to maximize bandwidth use and maintain quality of service.
2. **Security:** Security needs to exist throughout the network, from the routers to the computer, as part of Defense in Depth, "an integrated, multi-tiered security strategy." Information also needs to be shared across networks, and Cisco, Microsoft, and a third infrastructure vendor specializing in storage solutions—EMC—have been key players in producing off-the-shelf solutions using the secure information-sharing architecture (SISA) being used to share information between government departments in the United States.
3. **Management:** Network and system management becomes increasingly difficult as disparate systems are used—vendors now also act as system integrators to ensure a cohesive network is built.
4. **Wireless and Mobility:** While Cisco has a range of wireless VoIP products (e.g., the iPhone from subsidiary Linksys), Cisco does not have a presence in the cellular/mobile market. Cisco and Microsoft are working to extend the Unified Communications Manager to Windows Mobile devices.
5. **Unified Communications:** Microsoft takes a software-oriented approach to communications while Cisco views the network as "the hub of all communications," but the two companies will work together in some areas and compete to deliver unified communications solutions, ensuring interoperability, such as integrating MS Exchange server or MS Office Communications Server and Cisco Unified Communications Manager.
6. **Connected Entertainment:** Microsoft Media Centre provides the central PC facility while Cisco (under the Linksys and Scientific Atlanta customer premises equipment brands) produces "media extenders" that connect the PC to the TV and stereo, allowing the distribution of content around the home.
7. **Small and Medium Businesses:** Packaged solutions using combined solutions from both companies will be jointly marketed.

"Tell Us Your Business Challenge" Connects to Entrepreneurs

Each week, *Business Solutions,* sponsored by Cisco, answers a problem common to many entrepreneurs. They state: "If your business is facing a challenge, please send it, along with contact information, to *solutions@nationalpost.com*. You and your business could be featured in a future Business Solutions." In addition, Cisco offers helpful business tools at *financialpost.com/solutions*. For example, one challenge was: How do you manage and secure data in a cost-effective manner? Responses are posted as learning experiences for all. Another support for entrepreneurs is Cisco networking solutions, which helps them improve their small business with technology they can trust (see *cisco.com/ca/smb*).

Conclusion: Cisco's Strategy Is Serving Customers' Needs

Organizations of all sizes, in every industry, and throughout the world rely on networking technology to improve and protect business performance. Basic ways to improve or protect performance include a combination of the following:

- Increasing productivity of workers
- Reducing labor costs, product costs, service costs, or maintenance costs
- Collaborating with supply chain partners to reduce costs or delivery times
- Reducing time-to-market of new products or services
- Creating new revenue sources
- Responding to customers' needs or actions in real-time or near real-time
- Correcting operational problems quickly

- Responding quickly to competitive opportunities and threats
- Complying with regulators' requirements, such as protecting the confidential data of customers, employees, and business partners
- Providing secure, real-time visibility of the status of CRM, ERP, and supply chain systems

Cisco is leading the transition to intelligent network environments. Its success has resulted from continuously planning three to five years ahead of important market transitions. As Chambers said, "Historically, the transitions we've been a part of have been technological; they've been relatively orderly and predictable. Now, however, we're seeing a wider-reaching, more dramatic transition. So our ability to predict successfully where the market will go is even more critical and offers much greater potential import for the company."

References

"Alliances Keeps Network Management Specialist Moving up the Application Stack," *Manufacturing Business Technology*, 25(7), July 2007.

Dilger, K., "NetFlow-Infused Systems Watch for Trending, Traffic Patterns, Network Abnormalities," *Manufacturing Business Technology,* 26(5), May 2008.

Duffy, J., "Q&A: Cisco's CTO Talks First Impressions," *Network World,* 25(26), June 30, 2008.

Hoover's Company Records—In-depth Records, July 8, 2008.

Hoover's Company Records—Basic Record, July 22, 2008.

Silver, S., "In the Battle with Cisco, Tiny Nortel Plays Energy Card," *The Globe and Mail* (Canada), June 16, 2008.

White, B., "Brocade to Buy Foundry for Almost $3 Billion," *The Wall Street Journal,* July 22, 2008.

Questions

1. How does Cisco maintain its market dominance?
2. Identify three ways in which Cisco helps its business customers improve their business performance? (Chapters 3 and 4).
3. What products or services are provided by Cisco to support each of the following: business continuity, security, knowledge sharing, and collaboration? (Chapters 3, 4, and 5).
4. Review Table PII.2 showing Cisco's acquisitions during 2007 and 2008. Map the capabilities acquired to the categories in Table 4.5 in Chapter 4. How many of the acquired technologies are considered most likely to provide business value? What percent is that of the total number of acquired technologies?
5. Explain this statement: Competing companies, Cisco and Microsoft, are collaborating because of convergence. (Chapter 4).
6. What value does Cisco offer to entrepreneurs? To SMBs?
7. What security support does Cisco provide? (Chapter 5).
8. How does Cisco help its customers improve their performance?
9. How important was prediction to Cisco's former success? How important is prediction to Cisco's current and future success? Explain the difference.
10. Extra credit: Cisco has been a remarkably successful networking company. How would you categorize the company today? That is, is Cisco still primarily a networking company? Visit *cisco.com* for a current view of the company. Explain your answer.