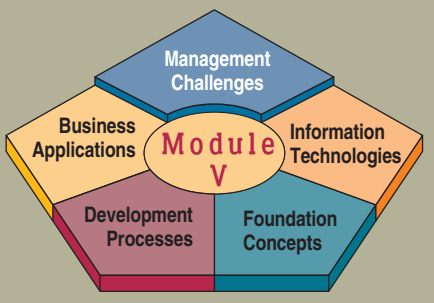
MODULE V

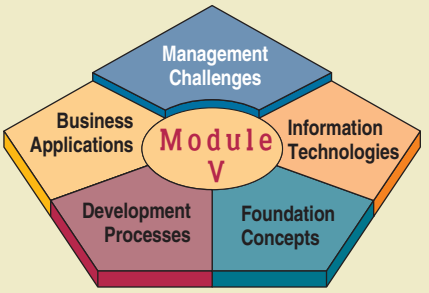


MANAGEMENT CHALLENGES

What managerial challenges do information systems pose for today's business enterprises? The two chapters of this module emphasize how managers and business professionals can manage the successful use of information technologies in a global economy.

- **Chapter 13: Security and Ethical Challenges** discusses the threats against and defenses needed for the performance and security of business information systems, as well as societal impact and ethical implications of information technology.
- **Chapter 14: Enterprise and Global Management of Information Technology** discusses the major challenges that information technology presents to business managers, the components of information systems management, and the managerial implications of the use of information technology in global business.

CHAPTER 13



SECURITY AND ETHICAL CHALLENGES

Chapter Highlights

Section I
Security, Ethical, and Societal Challenges of IT

Introduction
Ethical Responsibility of Business Professionals
Real World Case: Texas Health Resources and Intel: Ethics, IT, and Compliance
Computer Crime
Privacy Issues
The Current State of Cyber Law
Other Challenges
Health Issues
Societal Solutions

Section II
Security Management of Information Technology

Introduction
Tools of Security Management
Real World Case: Wyoming Medical Center, Los Angeles County, and Raymond James: End-Point Security Gets Complicated
Inter-Networked Security Defenses
Viral Defenses
Other Security Measures
System Controls and Audits
Real World Case: Ethics, Moral Dilemmas, and Tough Decisions: The Many Challenges of Working in IT
Real World Case: Raymond James Financial, BCD Travel, Houston Texans, and Others: Worrying about What Goes Out, Not What Comes In

Learning Objectives

1. Identify several ethical issues regarding how the use of information technologies in business affects employment, individuality, working conditions, privacy, crime, health, and solutions to societal problems.
2. Identify several types of security management strategies and defenses and explain how they can be used to ensure the security of business applications of information technology.
3. Propose several ways that business managers and professionals can help lessen the harmful effects and increase the beneficial effects of the use of information technology.

SECTION I Security, Ethical, and Societal Challenges of IT

Introduction

There is no question that the use of information technology in business presents major security challenges, poses serious ethical questions, and affects society in significant ways. Therefore, in this section, we explore the threats to businesses and individuals as a result of many types of computer crime and unethical behavior. In Section II, we will examine a variety of methods that companies use to manage the security and integrity of their business systems. Now let's look at a real-world example.

Read the Real World Case on the next page. We can learn a lot from this case about the security and ethical issues that result from the pervasive use of IT in organizations and society today. See Figure 13.1.

Business/IT Security, Ethics, and Society

The use of information technologies in business has had a major impact on society and thus raises ethical issues in the areas of crime, privacy, individuality, employment, health, and working conditions. See Figure 13.2.

It is important to understand that information technology has had beneficial results, as well as detrimental effects, on society and people in each of these areas. For example, computerizing a manufacturing process may have the beneficial result of improving working conditions and producing products of higher quality at lower cost, but it also has the adverse effect of eliminating people's jobs. So your job as a manager or business professional should involve managing your work activities and those of others to minimize the detrimental effects of business applications of information technology and optimize their beneficial effects. That would represent an ethically responsible use of information technology.

Ethical Responsibility of Business Professionals

As a business professional, you have a responsibility to promote ethical uses of information technology in the workplace. Whether or not you have managerial responsibilities, you should accept the ethical responsibilities that come with your work activities. That includes properly performing your role as a vital human resource in the business systems you help develop and use in your organization. As a manager or business professional, it will be your responsibility to make decisions about business activities and the use of information technologies that may have an ethical dimension that must be considered.

For example, should you electronically monitor your employees' work activities and e-mail? Should you let employees use their work computers for private business or take home copies of software for their personal use? Should you electronically access your employees' personnel records or workstation files? Should you sell customer information extracted from transaction processing systems to other companies? These are a few examples of the types of decisions you will have to make that have an ethical dimension. So let's take a closer look at several **ethical foundations** in business and information technology.

Business Ethics

Business ethics is concerned with the numerous ethical questions that managers must confront as part of their daily business decision making. For example, Figure 13.3 outlines some of the basic categories of ethical issues and specific business practices that have serious ethical consequences. Notice that the issues of intellectual property rights, customer and employee privacy, security of company records, and workplace safety are highlighted because they have been major areas of ethical controversy in information technology.

How can managers make ethical decisions when confronted with business issues such as those listed in Figure 13.3? Several important alternatives based on theories of

REAL WORLD CASE 1

Texas Health Resources and Intel: Ethics, IT, and Compliance

LUTTRELL, SONYA LOUISE 2566BU

The IT staff at Texas Health Resources Inc. must deliver more than technical functionality. And it needs to deliver more than the business requirements: It also has to meet the organization's ethical standards.

To that end, its systems must help ensure that Texas Health complies with laws and regulations.

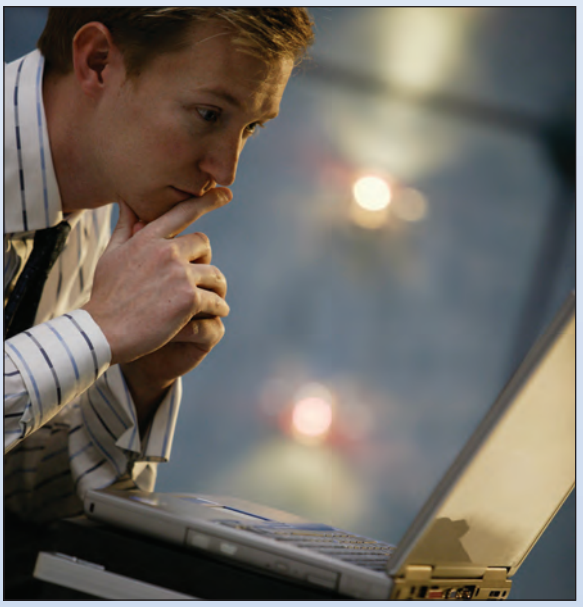
And they also have to promote the right behaviors and prevent or flag undesirable ones, says Michael Alverson, vice president and deputy CIO at the Arlington-based nonprofit health care system. Consider the challenge of handling patients' medical records. Even though the federal Health Insurance Portability and Accountability Act mandates that agencies keep those records private, caregivers still need to access them—when appropriate.

So the organization's electronic health records system "gives doctors and nurses who are caring directly for patients quick access when they use the right authentication," Alverson says.

But additional authentication is required to get records for patients who aren't under the provider's immediate care. The system records who gets access to what, allowing officials to audit and review cases to ensure there's no inappropriate access.

"The IT staff holds itself to similar ethical standards, too," Alverson says. The department has policies that prohibit taking gifts and endorsing vendors, to help guarantee that workers make procurement decisions based only on quality and needs.

FIGURE 13.1



The pervasive use of information technology in organizations and society presents individuals with new ethical challenges and dilemmas.

Source: © Punchstock.

And when there's any question—such as when a vendor proposes a deep discount if Texas Health agrees to be an early adopter of new technology—IT leaders can turn to the systemwide Business and Ethics Council for guidance.

"If we really want everyone to subscribe to the idea that working at Texas Health is special, then we have to have people actively believe in doing the right thing," Alverson says.

Companies are increasingly looking at their ethics policies and articulating specific values that address a range of issues, from community commitment to environmental sustainability, which employees can use to guide their work. The need to comply with federal laws and regulations drives some of this, while consumer expectations, employee demands and economic pressures also play a part.

Information technology consultant Dena L. Smith lays out a hypothetical dilemma: Should an IT department hire a more expensive vendor because the vendor shares its own company's ethics standards, or should it go with a lower-cost provider that doesn't?

Companies with established ethical standards that guide how they conduct business frequently confront this kind of question, Smith says, but it's a particularly tough question today, given the recession. With IT departments forced to cut budgets and staff, CIOs will find it difficult to allocate dollars for applications that promote corporate ethics.

"The decisions were easier in the days when the economics were favorable, but the choices may have to be more limited now," says former CIO John Stevenson, president of consultancy JG Stevenson Associates. "Now it's how much can you afford to do versus how much do you have to do so you don't get burned." Stevenson says companies that had moved toward certain ethical goals before the economic crisis—whether those goals involved green initiatives or corporate responsibility programs—aren't giving up their gains. "But if they haven't done that yet, it gets more difficult to say we'll spend more money than we have to," he says.

"Companies use the term 'corporate ethics' to mean many different things. In many organizations, if not the majority, it means compliance with a set of legal and minimum standards. In other organizations, corporate ethics means defining a set of corporate values that are integral to how they go about business," says Kirk O. Hanson, executive director of the Markkula Center for Applied Ethics at Santa Clara University.

Either way, CIOs have an opportunity to show how technology can further their companies' ethics objectives.

"Policy decisions at the very senior level need the sensitivity that IT experts can bring to the table," Hanson says. "CIOs will know the capabilities of IT and be able to contribute that to corporate strategy. They will also know the misuses of those capabilities and be able to flag those and prevent the organization from stepping in scandals."

Hanson cites a 15-year-old case in which marketing workers at a large telephone company spent millions of dollars to develop a list of customers with ties to the Washington

area that they planned to sell to other marketers. In violation of company policy, they compiled the list using the company's database of customers who frequently placed calls to the District of Columbia.

Executives learned about the list before the marketing department sold it. IT then developed a system to monitor use and block future unauthorized access to such information, Hanson says. However, it came a bit late, since IT should have developed the application in advance, anticipating the need to protect the information as well as detect any efforts to breach it.

Hanson says IT today can build systems that can screen potential subcontractors and vendors to see if they share certain values.

It's also possible to create tools that flag contracts whose costs exceed expectations in ways that suggest bribery or other improprieties, or set up systems that analyze customer satisfaction surveys to find evidence of unethical behaviors on the part of workers.

Meanwhile, companies that put green initiatives at the top of their ethical concerns can have IT create applications that track energy consumption to flag anomalies that indicate inefficiencies or calculate the corporate carbon footprint and identify ways to reduce it.

"You have to step back a minute and ask, 'What is the role of technology around ethics?'" says Smith. "Technology can help from a monitoring, protection and prevention standpoint in a lot of ways." The notion of corporate ethics hasn't always been so broad, says Mike Distelhorst, a law professor at Capital University Law School, a former adjunct professor of business ethics at the Capital School of Management and Leadership and former executive director for the university's Council for Ethical Leadership.

"You'd be hard-pressed to find any company that doesn't have a beautiful ethics and compliance program," Distelhorst says. "They're talking about it and they're working it all out in various strategic documents. But the question is whether they're actually living by it. Some are, and clearly some aren't."

Regardless of where a company stands in the process, IT leaders should be ready to contribute, he says.

"These policies are worked out on the ethics and compliance committees below the board level, and they're having the CIO as a key player," Distelhorst explains.

That's the case at Intel Corp., says the company's CIO, Diane Bryant.

Intel's Ethics and Compliance Oversight Committee established the following five principles for the company and its workers: Intel should conduct business with honesty and integrity; the company must follow the letter and spirit of the law; employees are expected to treat one another fairly; employees should act in the best interests of Intel and avoid conflicts of interest; and employees must protect the company's assets and reputation.

"Intel's IT staff builds and maintains the systems that allow the company to meet its legal and regulatory requirements. Such as those laid out for accounting and governance by the Sarbanes-Oxley Act," Bryant says.

It also developed applications and a team of workers to handle document retention, which is crucial should there be a legal case with electronic discovery requests.

But IT also enables Intel to enforce its own values and not just meet regulatory requirements, Bryant explains. So there are applications to help perform rigorous checks on suppliers to ensure that they have sufficient business continuity plans and environmental sustainability plans, as well as ethical stances that match Intel's own. IT has also delivered sophisticated systems that monitor the power consumption and carbon dioxide emissions of Intel's data centers. And it developed systems that monitor for potential malicious behavior, such as violations of access management rights or the public release of Intel's intellectual property.

"We put solutions in place that help protect Intel's five principles," Bryant says.

Few companies are that advanced in their use of technology to further an ethical agenda. "Companies recognize that they have to be on record as being committed, but they're not yet as convinced that they have to manage it like other parts of their business," Hanson explains.

But when companies do decide to move in that direction, that's when CIOs can shine, offering ideas on what metrics to use and what to measure.

"That's where IT can be a real leader," Hanson says, "since they know what can be measured and captured."

Source: Adapted from Mary K. Pratt, "Business Ethics Steering Clear of Scandal," *Computerworld*, August 23, 2009; and Mary K. Pratt, "The High Cost of Ethics Compliance," *Computerworld*, August 24, 2009.

LUTTRELL'S SONYA LOUISE 256 6BU

CASE STUDY QUESTIONS

1. What are the two meanings of 'corporate ethics' in organizations today? What does each definition imply for IT practices? How does the economic environment affect this?
2. How does IT provide more opportunities for difficult ethics issues to arise? How does IT help address those?
3. Use examples from the case to justify your answer.
4. Should organizations pursue high ethical standards regardless (or in spite of) their bottom-line impact? Or should they limit themselves to those scenarios where "good ethics make for good business"?

REAL WORLD ACTIVITIES

1. The passage of the Sarbanes-Oxley Act in the United States has greatly increased the compliance obligations of publicly traded companies. Go online to research how this landmark legislation affected the obligations of IT departments, and the way in which they develop and implement new technologies. Prepare a presentation to synthesize your findings.
2. Should an IT department hire a more expensive vendor because the vendor shares its own company's ethics standards, or should it go with a lower-cost provider that doesn't? This is an important question posed in the case above. What do you think? Break into small groups with your classmates to discuss your positions. Can you reach a consensus on this issue?

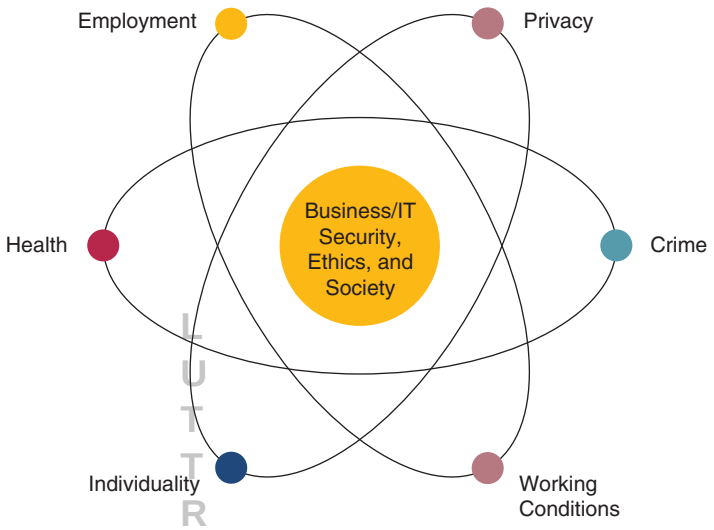


FIGURE 13.2
Important aspects of the security, ethical, and societal dimensions of the use of information technology in business. Remember that information technologies can support both beneficial and detrimental effects on society in each of the areas shown.

corporate social responsibility can be used. For example, in business ethics, the *stockholder theory* holds that managers are agents of the stockholders, and their only ethical responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices.

However, the *social contract theory* states that companies have ethical responsibilities to all members of society, which allows corporations to exist according to a social contract. The first condition of the contract requires companies to enhance the economic satisfaction of consumers and employees. They must do that without polluting the environment or depleting natural resources, misusing political power, or subjecting their employees to dehumanizing working conditions. The second condition requires companies to avoid fraudulent practices, show respect for their employees as human beings, and avoid practices that systematically worsen the position of any group in society.

The *stakeholder theory* of business ethics maintains that managers have an ethical responsibility to manage a firm for the benefit of all its stakeholders, that is, all individuals and groups that have a stake in, or claim on, a company. These stakeholders

FIGURE 13.3 Basic categories of ethical business issues. Information technology has caused ethical controversy in the areas of intellectual property rights, customer and employee privacy, security of company information, and workplace safety.

Equity	Rights	Honesty	Exercise of Corporate Power
Executive salaries	Corporate due process	Employee conflicts of interest	Product safety
Comparable worth	Employee health screening	**Security of company information**	Environmental issues
Product pricing	**Customer privacy**	Inappropriate gifts	Disinvestment
Intellectual property rights	**Employee privacy**	Advertising content	Corporate contributions
Noncompetitive agreements	Sexual harassment	Government contract issues	Social issues raised by religious organizations
	Affirmative action	Financial and cash management procedures	Plant/facility closures and downsizing
	Equal employment opportunity	Questionable business practices in foreign countries	Political action committees
	Shareholder interests		**Workplace safety**
	Employment at will		
	Whistle-blowing		

FIGURE 13.4
Ethical principles to help evaluate the potential harms or risks of the use of new technologies.

Principles of Technology Ethics
• **Proportionality.** The good achieved by the technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk.
• **Informed Consent.** Those affected by the technology should understand and accept the risks.
• **Justice.** The benefits and burdens of the technology should be distributed fairly. Those who benefit should bear their fair share of the risks, and those who do not benefit should not suffer a significant increase in risk.
• **Minimized Risk.** Even if judged acceptable by the other three guidelines, the technology must be implemented so as to avoid all unnecessary risk.

usually include the corporation's stockholders, employees, customers, suppliers, and the local community. Sometimes the term is broadened to include all groups who can affect or be affected by the corporation, such as competitors, government agencies, and special-interest groups. Balancing the claims of conflicting stakeholders is obviously not an easy task for managers.

Technology Ethics

Another important ethical dimension deals specifically with the ethics of the use of any form of technology. For example, Figure 13.4 outlines four principles of technology ethics. These principles can serve as basic ethical requirements that companies should meet to help ensure the ethical implementation of information technologies and information systems in business.

One common example of technology ethics involves some of the health risks of using computer workstations for extended periods in high-volume data entry job positions. Many organizations display ethical behavior by scheduling work breaks and limiting the exposure of data entry workers to staring at a computer monitor to minimize their risk of developing a variety of work-related health disorders, such as hand or eye injuries. The health impact of information technology is discussed later in this chapter.

Ethical Guidelines

We have outlined a few ethical principles that can serve as the basis for ethical conduct by managers, end users, and IS professionals. But what more specific guidelines might help your ethical use of information technology? Many companies and organizations answer that question today with detailed policies for ethical computer and Internet usage by their employees. For example, most policies specify that company computer workstations and networks are company resources that must be used only for work-related uses, whether using internal networks or the Internet.

Another way to answer this question is to examine statements of responsibilities contained in codes of professional conduct for IS professionals. A good example is the code of professional conduct of the Association of Information Technology Professionals (AITP), an organization of professionals in the computing field. Its code of conduct outlines the ethical considerations inherent in the major responsibilities of an IS professional. Figure 13.5 is a portion of the AITP code of conduct.

Business and IS professionals can live up to their ethical responsibilities by voluntarily following such guidelines. For example, you can be a **responsible professional** by (1) acting with integrity, (2) increasing your professional competence, (3) setting high standards of personal performance, (4) accepting responsibility for your work, and (5) advancing the health, privacy, and general welfare of the public. Then you would be demonstrating ethical conduct, avoiding computer crime, and increasing the security of any information system you develop or use.

FIGURE 13.5
Part of the AITP standards of professional conduct. This code can serve as a model for ethical conduct by business end users as well as IS professionals.

AITP Standards of Professional Conduct

In recognition of my obligation to my employer I shall:

- Avoid conflicts of interest and ensure that my employer is aware of any potential conflicts.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

In recognition of my obligation to society I shall:

- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, ensure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or a situation of public concern, nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner to achieve personal gain.

Source: 2007 PricewaterhouseCoopers Global Security Survey.

Enron Corporation: Failure in Business Ethics

Much has been said about the driven, cultlike ethos of the organization that styled itself "the world's leading company." Truth be told, for all its razzle-dazzle use of Internet technology, a lot of the things Enron did weren't so very exceptional: paying insanely large bonuses to executives, for example, often in the form of stock options (a practice that not only hid true compensation costs but also encouraged managers to keep the stock price up by any means necessary); promising outlandish growth, year after year, and making absurdly confident predictions about every new market it entered, however untested; scarcely ever admitting a weakness to the outside world; and showing scant interest in the questions or doubts of some in its own ranks about its questionable, unethical, and even illegal business and accounting practices.

Credibility comes hard in business. You earn it slowly by conducting yourself with integrity year in and year out, or by showing exceptional leadership in exceptional circumstances, such as on September 11, 2001. The surest way to lose it, short of being caught in an outright lie, is to promise much and deliver little. Those, at least, are two conclusions suggested by an exclusive survey of executives that Clark, Martire, and Bartolomeo conducted for *Business 2.0*.

Executives rated Enron Chairman and CEO Ken Lay least credible of the business figures in the survey. Perhaps it had something to do with statements like:

- "Our performance has never been stronger; our business model has never been more robust; our growth has never been more certain . . . I have never felt better about the prospects for the company."—E-mail to employees, August 14, 2001
- "The company is probably in the strongest and best shape that it has ever been in."—Interview in *BusinessWeek*, August 24, 2001
- "Our 26 percent increase in [profits] shows the very strong results of our core wholesale and retail energy businesses and our natural gas pipelines."—Press release, October 16, 2001

Yet three weeks later, Enron admitted that it had overstated earnings by $586 million since 1997. Within a few more weeks, Enron also disclosed a stunning $638 million third-quarter loss and then filed for Chapter 13 bankruptcy.

Dick Hudson, former CIO of Houston-based oil drilling company Global Marine Inc. and now president of Hudson & Associates, an executive IT consulting firm in Katy, Texas, thinks Enron started with a good business strategy and that if it hadn't pushed the envelope, it could well have been a successful Fortune 1000 firm. Instead, it aimed for the Fortune 10, so it got into markets such as broadband, which is a tough nut to crack even for the industry's leaders. "Those good old boys in Houston, they had to walk with the big dogs," accuses Hudson. "They are a textbook case of greed and mismanagement."

On May 25, 2006, Kenneth Lay was convicted on six counts of securities and wire fraud and faced a total of 45 years in prison. Lay died on July 5, 2006, before sentencing could be passed. His protege, Jeffrey K. Skilling, was convicted of 19 of 28 counts, and was sentenced to 24 years in prison. Andrew S. Fastow, the former chief financial officer, was sentenced to six years in prison for his role in the conspiracy that led to the collapse of Enron. His former lieutenant, Michael Kopper, received a reduced sentence of 37 months for cooperating with the investigation.

Source: Adapted from Melissa Solomon and Michael Meehan, "Enron Lesson: Tech Is for Support," *Computerworld*, February 18, 2002.

Computer Crime

Cyber-crime is becoming one of the Net's growth businesses. Today, criminals are doing everything from stealing intellectual property and committing fraud to unleashing viruses and committing acts of cyberterrorism.

Computer crime, a growing threat to society, is caused by the criminal or irresponsible actions of individuals who are taking advantage of the widespread use and vulnerability of computers and the Internet and other networks. It presents a major challenge to the ethical use of information technologies. Computer crime also poses serious threats to the integrity, safety, and survival of most business systems and thus makes the development of effective security methods a top priority. See Figure 13.6.

Computer crime is defined by the Association of Information Technology Professionals (AITP) as including (1) the unauthorized use, access, modification, and destruction of hardware, software, data, or network resources; (2) the unauthorized release of information; (3) the unauthorized copying of software; (4) denying an end user access to his or her own hardware, software, data, or network resources; and (5) using or conspiring to use computer or network resources to obtain information or tangible property illegally. This definition was promoted by the AITP in a Model Computer Crime Act and is reflected in many computer crime laws.

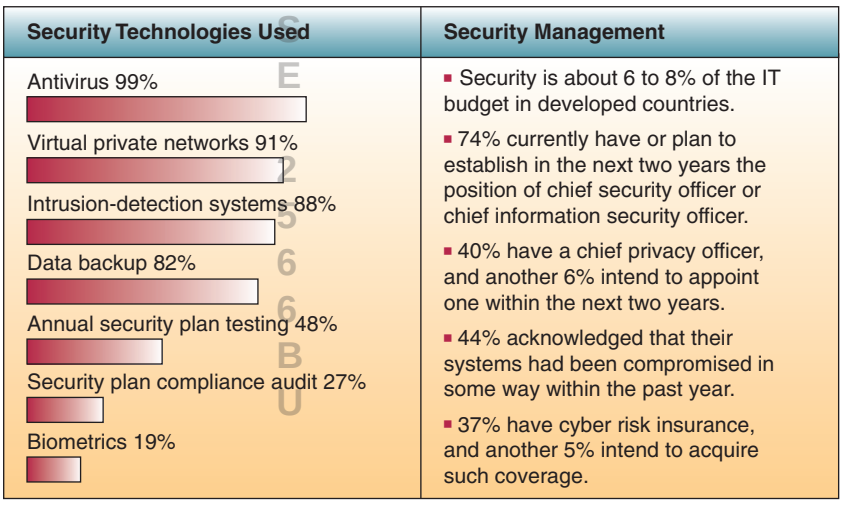


FIGURE 13.6
How large companies are protecting themselves from cyber-crime.

Source: 2007 PricewaterhouseCoopers Global Security Survey.

The Online Crusade against Phishing

Until just a few years ago, Gary Warner did not have the kind of day job you'd expect from an antiphishing crusader. He didn't work for a security vendor or a bank, or any kind of company you'd expect to care about phishing. Warner's career as a cyber-sleuth began on Halloween 2000. That's when his company's Web site was defaced by an entity named Pimpshiz as part of a pro-Napster Internet graffiti campaign.

"My boss came to me and said, 'Find out who did this and put them in jail,'" said Warner, who was at the time an IT staffer with Energen, a Birmingham, Alabama, oil and gas company. It was an eye-opening experience. "I called the police and they were like, 'What do you want us to do?'" he said. Months later, when Pimpshiz struck servers at NASA, Warner reached out, calling staff there and saying "Hey, we know who this guy is. Here's his name and address."

Since then, Warner has quietly become one of the most-respected authorities on phishing in the United States—the kind of guy that federal agents and banking IT staff call when they want to know how to catch the bad guys and shut down their credit-card-stealing Web sites.

With Warner's help, authorities eventually arrested Pimpshiz, whose real name is Robert Lyttle, in connection with the defacements.

Warner said that the Pimpshiz case was formative, underlining how hard it is for law enforcement to catch the bad guys on the Internet. "The experience showed me that it's not that they don't care," Warner said. "Their hands are tied by the legal process."

In July of 2007, with recommendations from FBI and Secret Service agents, Warner took a job as Director of Research in Computer Forensics with the University of Alabama at Birmingham (UAB). He also began working with law enforcement, not only educating FBI and Secret Service agents on how crimes were committed, but also helping to track down the criminals and helping with takedowns.

For Warner, the work isn't so much a job, as it is his moral responsibility as a computer scientist. "One of the things that really bothered me from the very beginning was people who were using my field to attack other people," he said. "The way I see it, this is our Internet. I'm going to stand at the end of my driveway and protect what's mine."

Warner is now focusing on fighting cyber-crime full-time and on training a new generation of network forensics investigators.

"You wouldn't believe the looks on their eyes the first time they got an e-mail back from a Webmaster saying, 'Thanks for letting me know. I just shut that down.'" Five days after final exams at the University of Alabama at Birmingham and though it would have no effect on their grades, four students were still coming into the labs to help shut down phishers.

"That idea that as a private citizen, you can help, that's the kind of thing we're trying to inspire," he says.

Source: Adapted from Robert McMillan, "Crime and Punishment: The White Knight of Phish-Busting," *Computerworld*, December 31, 2007.

JUSTICE SYNOPSIS

Hacking and Cracking

Cyber-thieves have at their fingertips a dozen dangerous tools, from "scans" that ferret out weaknesses in Web site software programs to "sniffers" that snatch passwords.

Hacking, in computerese, is the obsessive use of computers or the unauthorized access and use of networked computer systems. Hackers can be outsiders or company employees who use the Internet and other networks to steal or damage data and programs. One of the issues in hacking is what to do about a hacker who commits only *electronic breaking and entering*, that is, gets access to a computer system and reads some files but neither steals nor damages anything. This situation is common in computer crime cases that are prosecuted. In most cases, courts have found that the typical computer crime statute language prohibiting malicious access to a computer system did apply to anyone gaining unauthorized access to another's computer networks. See Figure 13.7.

2 SECOND REPLAY

FIGURE 13.7
Examples of common hacking tactics to assault companies through the Internet and other networks.

Common Hacking Tactics

Denial of Service. This is becoming a common networking prank. By hammering a Web site's equipment with too many requests for information, an attacker can effectively clog the system, slowing performance or even crashing the site. This method of overloading computers is sometimes used to cover up an attack.

Scans. Widespread probes of the Internet to determine types of computers, services, and connections. That way the bad guys can take advantage of weaknesses in a particular make of computer or software program.

Sniffer. Programs that covertly search individual packets of data as they pass through the Internet, capturing passwords or the entire contents.

Spoofing. Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers.

Trojan Horse. A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software.

Back Doors. In case the original entry point has been detected, having a few hidden ways back makes reentry easy—and difficult to detect.

Malicious Applets. Tiny programs, sometimes written in the popular Java computer language, that misuse your computer's resources, modify files on the hard disk, send fake e-mail, or steal passwords.

War Dialing. Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection.

Logic Bombs. An instruction in a computer program that triggers a malicious act.

Buffer Overflow. A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.

Password Crackers. Software that can guess passwords.

Social Engineering. A tactic used to gain access to computer systems by talking unsuspecting company employees out of valuable information such as passwords.

Dumpster Diving. Sifting through a company's garbage to find information to help break into their computers. Sometimes the information is used to make a stab at social engineering more credible.

Hackers can monitor e-mail, Web server access, or file transfers to extract passwords, steal network files, or plant data that will cause a system to welcome intruders. A hacker may also use remote services that allow one computer on a network to execute programs on another computer to gain privileged access within a network. Telnet, an Internet tool for interactive use of remote computers, can help hackers discover information to plan other attacks. Hackers have used Telnet to access a computer's e-mail port, for example, to monitor e-mail messages for passwords and other information about privileged user accounts and network resources. These are just some of the typical types of computer crimes that hackers commit on the Internet on a regular basis. That's why Internet security measures like encryption and firewalls, as discussed in the next section, are so vital to the success of e-commerce and other e-business applications.

The hacking community is quick to make the distinction between hacking and cracking. A cracker (also called a black hat or darkside hacker) is a malicious or criminal hacker. This term is seldom used outside of the security industry and by some modern programmers. The general public uses the term *hacker* to refer to the same thing. In computer jargon, the meaning of *hacker* can be much more broad. The name comes from the opposite of white hat hackers.

Usually a cracker is a person who maintains knowledge of the vulnerabilities he or she finds and exploits them for private advantage, not revealing them to either the general public or the manufacturer for correction. Many crackers promote individual freedom and accessibility over privacy and security. Crackers may seek to expand holes in systems; any attempts made to patch software are generally to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, a cracker may work to cause damage maliciously or make threats to do so for blackmail purposes.

The term *cracker* was coined by Richard Stallman to provide an alternative to abusing the existing word *hacker* for this meaning. This term's use is limited (as is "black

hat") mostly to some areas of the computer and security field and, even there, is considered controversial. One group that refers to themselves as hackers consists of skilled computer enthusiasts. The other, and more common usage, refers to people who attempt to gain unauthorized access to computer systems. Many members of the first group attempt to convince people that intruders should be called crackers rather than hackers, but the common usage remains ingrained.

Cyber-Theft

Many computer crimes involve the theft of money. In the majority of cases, they are inside jobs that involve unauthorized network entry and fraudulent alteration of computer databases to cover the tracks of the employees involved. Of course, many computer crimes involve the use of the Internet. One early example was the theft of $11 million from Citibank in late 1994. Russian hacker Vladimir Levin and his accomplices in St. Petersburg used the Internet for an electronic break-in of Citibank's mainframe systems in New York. They then succeeded in transferring the funds from several Citibank accounts to their own accounts at banks in Finland, Israel, and California.

In most cases, the scope of such financial losses is much larger than the incidents reported. Companies don't usually reveal that they have been targets or victims of computer crime. They fear scaring customers and provoking complaints by shareholders. In fact, several British banks, including the Bank of London, paid hackers more than a half million dollars not to reveal information about electronic break-ins.

Cyberterrorism

Cyberterrorism is the leveraging of an organization's or government's computers and information, particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure. There are some that argue cyberterrorism is really a form of hacking or information warfare. They disagree with labeling it terrorism because of the unlikelihood of the creation of fear, significant physical harm, or death in a population using electronic means, considering current attack and protective technologies.

The National Conference of State Legislatures (NCSL) puts a much finer point on the definition of the term:

> *the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically.*

Cyberterrorism can have a serious large-scale influence on significant numbers of people. It can significantly weaken a country's economy, thereby denying it access to vital resources and making it more vulnerable to military attack. Cyberterror can also affect Internet-based businesses. Like bricks and mortar retailers and service providers, most Web sites that produce income (whether by advertising, monetary exchange for goods, or paid services) could stand to lose money in the event of downtime created by cybercriminals. As Internet businesses have increasing economic importance to countries, what is normally cyber-crime becomes more political and therefore "terror" related.

To date, there have been no reported cyber-attacks on the United States. There have, however, been several large-scale examples of cyberterrorism in other countries. One such example occurred in Romania when cyberterrorists illegally gained access to the computers controlling the life-support systems at an Antarctic research station, endangering the 58 scientists involved. However, the culprits were stopped before damage actually occurred. Mostly nonpolitical acts of sabotage have caused financial and other damage, as in a case where a disgruntled employee caused the release of untreated sewage into water in Maroochy Shire, Australia. Computer viruses have degraded or shut down some nonessential systems in nuclear power plants, but this is not believed to have been a deliberate attack.

More recently, in May 2007, Estonia was subjected to a mass cyber-attack in the wake of the removal of a Russian World War II war memorial from downtown Talinn. The attack was a distributed denial of service attack in which selected sites were bombarded with traffic in order to force them off-line; nearly all Estonian government

ministry networks, as well as two major Estonian bank networks, were knocked off-line; in addition, the political party Web site of Estonia's current Prime Minister Andrus Ansip featured a counterfeit letter of apology from Ansip for removing the memorial statue. Despite speculation that the attack had been coordinated by the Russian government, Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government participation. In January 2008, a man from Estonia was convicted for launching the attacks against the Estonian Reform Party Web site and fined.

Leaving Your Job? Don't Take Anything with You

Employees who sign a noncompete agreement when hired, then break the agreement by leaving to work for a competitor, might want to exercise a little extra caution. Ex-employers might be able to use the Computer Fraud and Abuse Act to prosecute those suspected of stealing company intellectual property. The Act, designed to protect government computers and punish hackers, has been amended and now applies to any computer connected to the Internet, says Gregory Trimarche, a partner at the influential law and lobbying firm Greenberg Traurig.

Sensitive data can range from detailed customer and employee contact lists to internal marketing material. Trimarche considers intellectual property and trade secrets to be information that derives "independent economic value" that's not "generally known or available to the general public or competitors." An employee's know-how or talent doesn't fall into this category, but the company phone list with extensions could.

It's Sergio Kopelev's job to collect the evidence. Kopelev, a computer forensic specialist at LECG, which provides independent testimony, analysis, and consulting services to resolve disputes, said, "70 percent of people have stolen key information from work." By looking at the metadata, employers can determine when a document was printed. "You can secure the file's metadata by right-clicking on files running Microsoft Windows within the properties, for example," he says. "You also can tell when documents are copied to a thumb or flash drive. When you look at the drive forensically, the fact that someone has copied documents to a thumb drive is seen."

There is operating system metadata, software-dependent metadata, some collected by the machine and others by the user. "The most pilfered items include e-mail, address books and contact lists and customer databases," notes Kopelev.

Aside from taking the ex-employee to court, what's the recourse for companies that have executives who leave to work at a competitor? Vengeful employers can start yanking back stock options. John Giovannone, corporate attorney and partner at Greenberg Traurig, said there's a growing trend to include a "claw-back provision" giving employers the right to terminate stock options under certain circumstances, or make the employee pay back the difference between the exercised option price and fair-market stock price.

Lawyers at Greenberg Traurig "routinely" include the Computer Fraud and Abuse Act in lawsuits brought against ex-employees who jump ship to a competitor, says Trimarche. In the past several years, he's used the statute a handful of times. "It's a new tool and just now coming into common use. When you have a new statute that gives you a powerful tool, it takes time for the legal community, including judges, to get comfortable with it."

Source: Adapted from Laurie Sullivan, "Companies Urged to Prosecute Ex-Employees for Bringing Info to Competitors," *InformationWeek*, May 29, 2006.

Unauthorized Use at Work

The **unauthorized use** of computer systems and networks can be called *time and resource theft*. A common example is unauthorized use of company-owned computer networks by employees. This use may range from doing private consulting or personal finances to playing video games to unauthorized use of the Internet on company networks. Network monitoring software, called *sniffers*, is frequently used to monitor

FIGURE 13.8
Internet abuses in the workplace.

Internet Abuses	Activity
General E-mail Abuses	Include spamming, harassments, chain letters, solicitations, spoofing, propagations of viruses/worms, and defamatory statements.
Unauthorized Usage and Access	Sharing of passwords and access into networks without permission.
Copyright Infringement/ Plagiarism	Using illegal or pirated software that costs organizations millions of dollars because of copyright infringements. Copying of Web sites and copyrighted logos.
Newsgroup Postings	Posting of messages on various non-work–related topics from sex to lawn care advice.
Transmission of Confidential Data	Using the Internet to display or transmit trade secrets.
Pornography	Accessing sexually explicit sites from workplace as well as the display, distribution, and surfing of these offensive sites.
Hacking	Hacking of Web sites, ranging from denial of service attacks to accessing organizational databases.
Non-Work–Related Download/Upload	Propagation of software that ties up office bandwidth. Use of programs that allow the transmission of movies, music, and graphical materials.
Leisure Use of the Internet	Loafing around the Internet, which includes shopping, sending e-cards and personal e-mail, gambling online, chatting, game playing, auctioning, stock trading, and doing other personal activities.
Usage of External ISPs	Using an external ISP to connect to the Internet to avoid detection.
Moonlighting	Using office resources such as networks and computers to organize and conduct personal business (side jobs).

Source: Adapted from Keng Siau, Fiona Fui-Hoon Nah, and Limei Teng, "Acceptable Internet Use Policy," *Communications of the ACM*, January 2002, p. 76.

network traffic to evaluate network capacity, as well as to reveal evidence of improper use. See Figure 13.8.

According to one survey, 90 percent of U.S. workers admit to surfing recreational sites during office hours, and 84 percent say they send personal e-mail from work. So this kind of activity alone may not get you fired from your job; however, other Internet activities at work can bring instant dismissal. For example, *The New York Times* fired 23 workers because they were distributing racist and sexually offensive jokes on the company's e-mail system.

Xerox Corp. fired more than 40 workers for spending up to eight hours a day on pornography sites on the Web. Several employees even downloaded pornographic videos, which took so much network bandwidth that it choked the company network and prevented coworkers from sending or receiving e-mail. Xerox instituted an eight-member SWAT team on computer abuse that uses software to review every Web site its 40,000 computer users view each day. Other companies clamp down even harder by installing software like SurfWatch, which enables them to block and monitor access to off-limit Web sites.

Survey: E-mail and Internet Abuse Can Get You Fired

Think you can get away with using e-mail and the Internet in violation of company policy? *Think again*. A new survey found that more than one-quarter of employers have fired workers for misusing e-mail, and one-third have fired workers for misusing the Internet on the job. The study, conducted by the American Management Association and the ePolicy Institute, surveyed 304 U.S. companies of all sizes.

The vast majority of bosses who fired workers for Internet misuse, 84 percent, said the employee was accessing porn or other inappropriate content. Although it is obviously wrong to look at inappropriate content on company time, a surprising number of people were fired just for surfing the Web. As many as 34 percent of managers in the study said they let go of workers for excessive personal use of the Internet, according to the survey.

Among managers who fired workers for e-mail misuse, 64 percent did so because the employee violated company policy and 62 percent said the workers' e-mail contained inappropriate or offensive language. More than a quarter of bosses said they fired workers for excessive personal use of e-mail, and 22 percent said their workers were fired for breaching confidentiality rules in e-mail.

Companies are worried about the inappropriate use of the Internet, and so 66 percent of those in the study said they monitor Internet connections. As many as 65 percent of them use software to block inappropriate Web sites. Eighteen percent of the companies block URLs (uniform resource locators) to prevent workers from visiting external blogs.

Companies use different methods to monitor workers' computers, with 45 percent of those participating in the survey tracking content, keystrokes, and time spent at the keyboard. An additional 43 percent store and review computer files. Twelve percent monitor blogs to track content about the company, and 10 percent monitor social-networking sites.

The researchers found that even though only two states require companies to notify their workers that they're monitoring them, most tell employees of their monitoring activities. Of the companies that monitor workers in the survey, 83 percent said they tell employees that they are monitoring content, keystrokes, and time spent at the keyboard. As many as 84 percent tell employees that they review computer activity, and 71 percent alert workers that they monitor their e-mails.

Source: Adapted from Nancy Gohring, "Over 50% of Companies Fire Workers for E-Mail, 'Net Abuse," *CIO Magazine*, February 28, 2008.

Software Piracy

Computer programs are valuable property and thus the subject of theft from computer systems. However, unauthorized copying of software, or **software piracy**, is also a major form of software theft. Software piracy by company employees is widespread, which has resulted in lawsuits by the Software Publishers Association, an industry association of software developers, against major corporations that allowed unauthorized copying of their programs.

Unauthorized copying is illegal because software is intellectual property that is protected by copyright law and user licensing agreements. For example, in the United States, commercial software packages are protected by the Computer Software Piracy and Counterfeiting Amendment to the Federal Copyright Act. In most cases, the purchase of a commercial software package is really a payment to license its fair use by an individual end user. Therefore, many companies sign *site licenses* that legally allow them to make a certain number of copies for use by their employees at a particular location. Other alternatives are *shareware*, which allows you to make copies of software for others, and *public domain software*, which is not copyrighted.

The most recent study by the Business Software Alliance, an antipiracy group whose members include Apple Computer, IBM, Intel, and Microsoft, shows that in 2007, pirated software accounts for 38 percent of software in use worldwide. Reported losses from software piracy in 2007 were almost $48 billion—up $8 billion from the year before. "That's over a third of the industry's revenue," says Bob Kruger, the group's vice president for enforcement. According to the findings, only $50 billion of the $100 billion in software purchased in 2007 was legally acquired. In other words, for every dollar

spent on software purchased legitimately worldwide, there was 50 cents' worth of software that was obtained illegally.

For example, Carol Bartz, the president and chairman of Autodesk, Inc. (www.autodesk.com) reports that one of their flagship products, AutoCAD, has 90 percent of the computer-aided design (CAD) market in China, yet sales are virtually negligible due to the widespread acceptance of software piracy. Bartz also states that many software companies are reluctant to pursue the educational market due to concerns that several copies of purchased software may lead to millions of copies of illegal software, produced "in the name of educating children."

Theft of Intellectual Property

Software is not the only property that is subject to computer-based piracy. Other **intellectual property theft** occurs in the form of infringements of copyrighted material, such as music, videos, images, articles, books, and other written works, which most courts have deemed illegal. Digitized versions can easily be captured by computer systems and made available for people to access or download at Internet Web sites or can be readily disseminated by e-mail as file attachments. The development of peer-to-peer (P2P) networking technologies (discussed in Chapter 6) has made digital versions of copyrighted material even more vulnerable to unauthorized use. For example, P2P file-sharing software enables direct MP3 audio file transfers of specified tracks of music between your PC and those of other users on the Internet. Thus, such software creates a *peer-to-peer network* of millions of Internet users who electronically trade digital versions of copyrighted or public domain music stored on their PC's hard drives. More recently, music publishers and manufacturers are offering legal, and relatively inexpensive, methods to access online music in a variety of formats. Because of this proactive posture, the music industry reports that illegal downloading of music and video properties is down and continuing to drop significantly. Let's look at the ongoing debate in this controversial area more closely with a real-world example that emphasizes the threat of developments in IT to intellectual property rights.

Music Piracy: The Long War

> *"Canadian pirates" is what the music dealers call publishing houses across the line who are flooding this country, they say, with spurious editions of the latest copyrighted popular songs. They use the mails [sic] to reach purchasers, so members of the American Music Publishers' Association assert, and as a result the legitimate music publishing business of the United States has fallen off 50 percent in the past twelve months. Their investigation has revealed that all of the most popular pieces have been counterfeited, despite the fact that they are copyrighted, and by unknown publishers are sold at from 2 cents to 5 cents per copy, though the original compositions sell at from 20 to 40 cents per copy.*

Sounds somewhat familiar? You may be a little too young to remember, but it was published in *The New York Times* sometime ago—June 13, 1897 to be exact. As you can see, music piracy is hardly a recent phenomenon. It has, however, reached staggering proportions in the last two decades or so, from Napster to torrents, and including the less sophisticated but widely available CD burners.

However, only a few years after Napster's launch, online song-swapping took a big hit from a dogged legal campaign by the Recording Industry Association of America (RIAA) to shut down the top services, Napster and Audiogalaxy. Others—like Kazaa and Morpheus—went on the run, as their users were being sued by the RIAA.

Other networks, like Gnutella, had been built to withstand legal assault. By avoiding centralized servers and spreading the goods around the globe, the free-music hackers hoped their networks would be impossible to shut down. Too bad they also became impossible to use. Shawn Fanning (the creator of Napster) had a hit because Napster provided quick and easy access to a huge trove of music. His deservedly nameless imitators required far more work to find far fewer tunes.

At times, the attention moved to the pirating and copying of physical CDs. Look at the numbers: Industry estimates say that more than 6 billion blank CDs were sold worldwide in 2003—that's one for every person alive today—along with 44 million drives on which to burn them. By 2004, worldwide sales of CD-Audio, CD-ROM, and CD-R all together surpassed 30 billion units. In addition, millions of people now own writable drives—far more than the most optimistic membership claims made by Napster or any of its heirs. "You'll find one on nearly every consumer PC," cites Gartner analyst Mary Craig, one of the more bearish forecasters in the business. "They're not using them for backups."

Today, peer-to-peer (P2P) torrent clients have spread broadly. LimeWire, a grizzled veteran of the peer-to-peer (P2P) file-sharing scene, remains the most popular software for exchanging music, video, and software—much of it pirated—through the Internet, with µTorrent a not-too-close second. LimeWire was used on 17.8 percent of PCs in September of 2007, according to a Digital Media Desktop Report. Since about half of surveyed PCs have at least one peer-to-peer sharing application installed, that gives LimeWire a 36.4 percent share—more than three times the 11.3 percent share of the next-most-popular client, µTorrent.

Source: Adapted from Paul Boutin, "Burn Baby Burn," *Wired*, December 2002; and Eric Lai, "Study: LimeWire Remains Top P2P Software; µTorrent Fast-Rising No. 2," *Computerworld*, April 17, 2008.

Computer Viruses and Worms

One of the most destructive examples of computer crime involves the creation of a **computer virus** or *worm*. *Virus* is the more popular term, but technically, a virus is a program code that cannot work without being inserted into another program. A worm is a distinct program that can run unaided. In either case, these programs copy annoying or destructive routines into the networked computer systems of anyone who accesses computers infected with the virus or who uses copies of magnetic disks taken from infected computers. Thus, a computer virus or worm can spread destruction among many users. Although they sometimes display only humorous messages, they more often destroy the contents of memory, hard disks, and other storage devices. See Figure 13.9.

Computer viruses typically enter a computer system through e-mail and file attachments via the Internet and online services or through illegal or borrowed copies of software. Copies of *shareware* software downloaded from the Internet can be another source of viruses. A virus usually copies itself into the files of a computer's operating system. Then the virus spreads to the main memory and copies itself onto the computer's hard disk and any inserted floppy disks. The virus spreads to other computers through e-mail, file transfers, other telecommunications activities, or floppy disks from infected computers. Thus, as a good practice, you should avoid using software from questionable sources without checking for viruses. You should also regularly use *antivirus programs* that can help diagnose and remove computer viruses from infected files on your hard disk. We will discuss defense against viruses further in Section II.

Oldies but Goodies: Old Threats That Just Won't Go Away

Worried about the virulent Storm worm that has been buffeting the Internet with mass mailings? Symantec Corp. researchers said that the "Storm Trojan," aka "Peacomm," is now spreading via AOL Instant Messenger (AIM), Google Talk, and Yahoo Messenger.

An alert to some Symantec customers pegged the new infection vector as "insidious" because the message—such as the cryptic "LOL;)"—and the included URL can be dynamically updated by the attacker. Even worse, according to Alfred Huger, senior director of Symantec's security response team, "it injects a message

(text continues on page 544)

FIGURE 13.9 The top five virus families of all time. Note that three of the five occurred during 2004.

Top Five Virus Families of All Time

MyDoom **First Discovered: 1/26/2004**

- Spreads both by e-mail and over the Kazaa file-sharing network. It appears to install some form of backdoor component on compromised machines, as well as effecting a denial of service attack on the SCO Group's Web site.
- The e-mail poses either as a returned message, or as a Unicode message that can't be rendered properly, and urges the target to click on the attachment to see the message.
- This worm also has a backdoor component, which opens up two TCP ports that stay open even after the worm's termination date (February 12, 2004).
- Upon executing the virus, a copy of Notepad is opened, filled with lots of nonsense characters.

Netsky **First Discovered: 3/3/2004**

- A mass-mailing worm that spreads by e-mailing itself to all e-mail addresses found in files on all local and mapped network drives.
- It also tries to spread via peer-to-peer file-sharing applications by copying itself into the shared folder used by the file-sharing applications (it searches for folders whose name contains the string "share" or "sharing"), renaming itself to pose as one of 26 other common files along the way.

SoBig **First Discovered: 6/25/2003**

- A mass-mailing e-mail worm that arrives in the form of an e-mail attachment named either "Movie_0074.mpeg.pif," "Document003.pif," "Untitled1.pif," or "Sample.pif." The message subject title will read either "Re: Movies," "Re: Sample," "Re: Document," or "Re: Here is that sample," and it will appear to originate from big@boss.com.
- The worm will scan all .WAB, .DBX, .HTML, .HTM, .EML, and .TXT files on the victim's machine looking for e-mail addresses to which it can send itself and attempts to spread over the local network.
- It will also attempt to download updates for itself.

Klez **First Discovered: 4/17/2002**

- A mass-mailing e-mail worm that arrives in the form of an e-mail attachment with a random file name. The worm exploits a known vulnerability in MS Outlook to autoexecute on unpatched clients. Once run, the worm will try to disable a selection of security applications—specifically virus scanners—and tries to copy itself to all local and networked drives, renaming itself with a random file name.
- Virus has a very damaging payload: It drops the W32/Elkern virus, which will delete all files it can find on the infected machine and any mapped network drives on the 13th of all even-numbered months.

Sasser **First Discovered: 8/24/2004**

- Spreads by exploiting a recent Microsoft vulnerability, spreading from machine to machine with no user intervention required.
- The worm spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The worm scans public ranges like 10.0.0.0 and 192.168.0.0 only if they are part of the local subnet.

The Cost of All This . . .

- Nearly 115 million computers across 200 countries were infected at one time or another in 2004 by rapidly proliferating software agents including Trojans, viruses, and worms.
- As many as 11 million computers worldwide—mostly within homes and small organizations—are now believed to be permanently infected and are used by criminal syndicates or malevolents to send out spam; mount distributed denial of service (DDoS) attacks; carry out extortion, identity theft, and phishing scams; or disseminate new viruses.
- The total economic damage worldwide from virus proliferation—with an additional 480 new species in 2004 alone—is now estimated to be between $166 billion and $202 billion for 2004 by the mi2g Intelligence Unit.
- With an installed base of around 600 million Windows-based computers worldwide, average damage per installed machine is between $277 and $336.

Source: Mi2g.com, "2004: Year of the Global Malware Epidemic—Top Ten Lesson," November 21, 2004.

and URL only into already open windows. It's not just some random message that pops up, but it appears only to people you are already talking to. That makes the approach very effective."

Well, you should be concerned about the Storm worm, but Gunter Ollmann, director of security strategy at IBM's Internet Security Systems, says the most common malware attack today is coming from the Slammer worm. *No, you didn't misread that last sentence*. The Slammer worm, which hit in January 2003, is still working its way around the Internet and within corporate networks, according to Ollmann. And it's still spreading in a big way. Slammer isn't the only piece of old-time malware that is still wreaking havoc.

"The stuff malware authors wrote a while ago is still out there and still propagating and still infecting machines," he said. "Some have more infections now than they did when they were headline news. All those old vulnerabilities haven't all gone away." Slammer, the worm that brought many networks to their knees by attacking Microsoft's SQL Server, is at the top of Ollmann's list of current malware problems.

"When we hear about the latest worm and zero-day, Slammer still beats them by a long shot," he added. "Slammer is still out there on a large number of infected hosts and it's still sending out malicious network traffic—malicious packets. . . . When people restore data after a crash, it probably is from an old system and it may not have the patches so it can easily be re-infected."

Another problem is that some users just don't do the patching they should, while other users aren't even aware that Microsoft SQL Server is running on their desktop because it's common to several other applications. If they don't know it's there, they don't know to take care of it.

"All these old viruses are never going to go away," said Ollmann.

Source: Adapted from Sharon Gaudin, "Oldies but Goodies: Slammer Worm Still Attacking," *InformationWeek*, August 24, 2007; and Gregg Keizer, "'Storm Trojan' Ignites Worm War," *Computerworld*, February 12, 2007.

Adware and Spyware

Two more recent entries into the computer vulnerabilities arena are **adware** and **spyware**. By definition, adware is software that, while purporting to serve some useful function and often fulfilling that function, also allows Internet advertisers to display advertisements as banners and pop-up ads without the consent of the computer user. In the extreme, adware can also collect information about the user of its host computer and send it over the Internet to its owner. This special class of adware is called **spyware** and is defined as any software that employs users' Internet connection in the background without their knowledge or explicit permission. Spyware programs collect specific information about you, ranging from general demographics like name, address, and Internet surfing habits to credit card, Social Security number, user names, passwords, or other personal information. It is important to understand that not all adware programs are spyware. Proper adware represents a viable, albeit sometimes irritating, revenue model for many software companies that allows you to get products for free and, when used correctly, does not pose any significant privacy threat. In contrast, spyware is and should be considered a clear threat to your privacy.

Whereas proper adware generally allows the computer user to opt in to its use in exchange for free use of a piece of software, spyware operates under a rather bizarre ethical model. Consider the following:

- You illegally enter a bank's computer system and place a stealth piece of software in their system. If you are detected or caught, you might be prosecuted and may go to jail.
- You write a worm or virus and spread it around the Internet or other networks. If you are detected or caught, you might be prosecuted and may go to jail.

- You write a program that spreads a spyware agent across computer systems connected to the Internet that steals the private information of the users it infects, manipulates their Internet experience, and uses other people's Web sites and browsers to display your advertising. If you are detected or caught, you may get rich, you don't go to jail, and the computer users are left with possibly rebuilding their computer system to get rid of your spyware.

Spyware has a variety of characteristics, beyond its potential for stealing valuable private information, which make it undesirable to most computer users. At the very least, it plagues the user of the infected machine with unwanted advertising. More often, it watches everything a user does online and sends that information back to the marketing company that created the spyware. Often, spyware applications add advertising links to Web pages owned by other people, for which the Web page owner does not get paid, and may even redirect the payments from legitimate affiliate-fee advertisers to the makers of the spyware. Other undesirable characteristics include setting an infected system's browser home page and search settings to point to the spyware owner's Web sites (generally loaded with advertising), often in a manner that prevents you from changing back the settings (referred to as home-page hijacking). In the extremes, spyware can make a dial-up modem continually call premium-rate phone numbers, thus causing large telephone charges (and usually fees to the spyware owner) or leave security holes in an infected system allowing the makers of the spyware—or, in particularly bad cases, anyone at all—to download and run software on the infected machine (such downloads are called *Trojans*). In almost all cases, spyware severely degrades system performance. As you can see, spyware doesn't have any redeeming features except for the benefits to its owner. Its use is pervasive, and failing to protect against it virtually ensures that your system will eventually become infected.

Protecting against adware and spyware generally requires the purchase and installation of one of a variety of programs designed to prevent the software from being downloaded and installed. Once a computer is infected, however, removal programs are often not completely successful in eliminating the nuisance.

Commtouch: Trends in Virus, Spam, and Phishing

Commtouch, a developer of technology for real-time antispam and virus protection, reports on a variety of spam and computer virus statistics on a periodic basis. Although new threats arise daily by the hundreds (if not thousands), just looking at a single quarter will provide you with an idea of what is constantly going on in this world. So here are some of the highlights from the first quarter of 2010:

A glitch in SpamAssassin, the most widely used free antispam software, at the beginning of 2010 resulted in false positives and rejection of legitimate mail. SpamAssassin is widely used by organizations, universities, and also vendors who integrate it into their own detection engines. The buggy parameter in the rule, clearly created many years ago, stated that messages from 2010 were "from the far future," and thus raising the false-positive ratio by as much as 20 percent.

During the first quarter of 2010, Commtouch analyzed which categories of Web sites were most likely to be compromised with malware or phishing. As expected and in line with the last several quarters, pornographic and sexually explicit sites ranked highest in the categories infected with malware. On the list of Web categories likely to be hosting hidden phishing pages, sites related to sex education ranked highest. These are followed by socially oriented sites such as games, chat, and social networking, which are easier targets for posting hidden phishing pages.

The lifespan of zombies (computers connected to the Internet that have been compromised by a hacker, a computer virus, or a trojan horse) is very short, and

according to Commtouch Labs, the first quarter saw an average turnover of 305,000 zombies each day that were newly activated for malicious activity, like sending malware and spam. Brazil continued to produce the most zombies with 14 percent of the overall count.

As part of Commtouch's analysis of spam trends, Commtouch Labs monitors the domains that are used by spammers in the "from" field of the spam e-mails. Naturally, the addresses are typically faked in order to fool antispam systems and to give the impression of a reputable, genuine source. Occasionally spammers will use a company name, for example, UPS—particularly when sending malware disguised as "UPS delivery information." The domain that is most often faked, however, is gmail.com.

Spam levels averaged 83 percent of all e-mail traffic throughout the quarter, peaking at nearly 92 percent near the end of March and bottoming out at 75 percent at the start of the year. Assuming worldwide e-mail traffic of about 220 billion e-mails per day, this would equate to an average of about 183 billion spam messages per day. The following table shows the most popular spam topics in the first quarter of 2010:

Category of Spam	% of Spam
Pharmacy	81.0
Replicas	5.4
Enhancers	2.3
Phishing	2.3
Degrees	1.3
Casino	1.0
Weight Loss	0.4
Other	6.3

Source: Commtouch, "Q1 2010 Internet Threats Trend Report," http://www.commtouch.com.

Privacy Issues

Information technology makes it technically and economically feasible to collect, store, integrate, interchange, and retrieve data and information quickly and easily. This characteristic has an important beneficial effect on the efficiency and effectiveness of computer-based information systems. The power of information technology to store and retrieve information, however, can have a negative effect on the **right to privacy** of every individual. For example, confidential e-mail messages by employees are monitored by many companies. Personal information is being collected about individuals every time someone visits a site on the World Wide Web. Confidential information on individuals contained in centralized computer databases by credit bureaus, government agencies, and private business firms has been stolen or misused, resulting in the invasion of privacy, fraud, and other injustices. The unauthorized use of such information has badly damaged the privacy of individuals. Errors in such databases could seriously hurt the credit standing or reputation of an individual.

Governments around the world, but none more than in the United States, are debating privacy issues and considering various forms of legislation. With regard to the Internet, **opt-in** versus **opt-out** is central to the debate over privacy legislation. Consumer protection groups typically endorse an opt-in standard, making privacy the default. An opt-in system automatically protects consumers who do not specifically allow data to be compiled about them. Most business interests back opt-out, arguing it doesn't disrupt the flow of e-commerce. Interestingly, current laws in this regard differ between the

United States and Europe. In the United States, opt-out is the default position, whereas in Europe, consumers must opt-in or their information cannot be used.

Additional privacy issues under debate include:

- Accessing private e-mail conversations and computer records and collecting and sharing information about individuals gained from their visits to Internet Web sites and newsgroups (violation of privacy).
- Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places (computer monitoring).
- Using customer information gained from many sources to market additional business services (computer matching).
- Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles (unauthorized personal files).

Privacy on the Internet

If you don't take the proper precautions, any time you send an e-mail, access a Web site, post a message to a newsgroup, or use the Internet for banking and shopping . . . whether you're online for business or pleasure, you're vulnerable to anyone bent on collecting data about you without your knowledge. Fortunately, by using tools like encryption and anonymous remailers—and by being selective about the sites you visit and the information you provide—you can minimize, if not completely eliminate, the risk of your privacy being violated.

The Internet is notorious for giving its users a feeling of anonymity when in reality they are highly visible and open to violations of their privacy. Most of the Internet and its World Wide Web, e-mail, chat, and newsgroups are still a wide open, unsecured electronic frontier, with no tough rules on what information is personal and private. Information about Internet users is captured legitimately and automatically each time you visit a Web site or newsgroup and is recorded as a "cookie file" on your hard disk. Then the Web site owners or online auditing services like DoubleClick may sell the information from cookie files and other records of your Internet use to third parties. To make matters worse, much of the Net and Web is an easy target for the interception or theft by hackers of private information furnished to Web sites by Internet users.

Of course, you can protect your privacy in several ways. For example, sensitive e-mail can be protected by encryption, if both e-mail parties use compatible encryption software built into their e-mail programs. Newsgroup postings can be made privately by sending them through *anonymous remailers* that protect your identity when you add your comments to a discussion. You can ask your Internet service provider not to sell your name and personal information to mailing list providers and other marketers. Finally, you can decline to reveal personal data and interests on online service and Web site user profiles to limit your exposure to electronic snooping.

Identity Theft: As Easy as Stealing a Check

Frank W. Abagnale Jr. was a check forger for five years in the 1960s. Currently he runs Abagnale and Associates, a financial fraud consultancy company. His life story provided the inspiration for the feature film *Catch Me If You Can*, starring Leonardo DiCaprio as Frank Abagnale Jr., as well as Tom Hanks.

Forty years ago, few people could have predicted that identity theft would become as big an epidemic as it is today. Few could have imagined that protecting your identity would mean taking mail to the post office instead of leaving it in our mailboxes for pickup, shredding documents before throwing them in the trash, or that a $2 pen could help prevent a crime.

"We need to find ways to protect ourselves before identity theft strikes. We can make drastic improvements toward diminishing this crime, but it will never disappear altogether. If you haven't been a victim of identity theft, it is because thieves haven't gotten to you yet. If things fail to change, your turn will come. Prevention is not simply a matter of following a checklist of tips, it is about education—the primary factor in protecting ourselves," says Frank W. Abagnale Jr.—and he should know.

Although more and more people are using online banking, America's 78 million baby boomers, who make up 15 percent of the U.S. population, continue to be a paper-driven majority. This group also accounts for 30 percent of fraud victims, as estimated by Consumer Action, a consumer-advocacy group.

"A check holds all of the information needed to steal your identity: name, address, bank account, routing number. If written with a ball point pen, information can easily be removed by a process called check washing, a common form of identity theft. It is the process of taking a check or document that has already been filled out, removing the ink with a regular household chemical, then re-writing in a new dollar amount and recipient," says Abagnale. If you are careless, your personal check could contribute to the 1.2 million fraudulent checks written every day. That's more than 13 per second.

The American Bankers Association states that check fraud is growing 25 percent per year. To slow this growth, it is important to understand how it works. "I know firsthand how easy it is to perform check fraud. About 40 years ago, I cashed $2.5 million in fraudulent checks in every state and 26 foreign countries over a five-year period. I was involved in a high-stakes game of stolen identities. And to know how easy it can be to perform, I know it is just as easy to prevent," he notes.

Criminals rely on our mistakes to make their job easier. Taking a few precautions will make you less attractive to predators. Don't leave mail in your mailbox overnight or over the weekend. When writing checks and filling out important documents, use a gel pen, so thieves can't remove the ink and change the information. In addition, shred or tear up unwanted documents that contain personal information before discarding them. The cost of a high-quality shredder is far less than the cost of having your identity stolen.

"Let's face it; we can't always control what is happening in our world, so we must take steps to control what we can. Technology is here to stay, but there are still simple and inexpensive ways to prevent identity theft when writing checks. Remember that a crook always looks for the easiest route to riches. Don't hand him a map. Be proactive and start protecting yourself today," says Abagnale.

Source: Adapted from Frank Abagnale, "Abagnale: Top Tips to Prevent Identity Theft and Fraud," *CIO Magazine*, May 24, 2007.

ETHICAL ISSUES

Computer Matching

Computer profiling and mistakes in the **computer matching** of personal data are other controversial threats to privacy. Individuals have been mistakenly arrested and jailed and people have been denied credit because their physical profiles or personal data have been used by profiling software to match them incorrectly or improperly with the wrong individuals. Another threat is the unauthorized matching of computerized information about you extracted from the databases of sales transaction processing systems and sold to information brokers or other companies. A more recent threat is the unauthorized matching and sale of information about you collected from Internet Web sites and newsgroups you visit, as we discussed previously. You are then subjected to a barrage of unsolicited promotional material and sales contacts as well as having your privacy violated.

Privacy Laws

Many countries strictly regulate the collection and use of personal data by business corporations and government agencies. Many government *privacy laws* attempt to enforce the privacy of computer-based files and communications. For example, in the

United States, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act prohibit intercepting data communications messages, stealing or destroying data, or trespassing in federal-related computer systems. Because the Internet includes federal-related computer systems, privacy attorneys argue that the laws also require notifying employees if a company intends to monitor Internet usage. Another example is the U.S. Computer Matching and Privacy Act, which regulates the matching of data held in federal agency files to verify eligibility for federal programs.

More recently, new legislation intended to protect individual privacy has created some new challenges for organizations. Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, the USA PATRIOT Act, the California Security Breach Law, and Securities and Exchange Commission rule 17a-4 are but a few of the compliance challenges facing organizations. In an effort to comply with these new privacy laws, it is estimated that a typical company will spend 3–4 percent of its IT budget on compliance applications and projects.

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. It is a broad piece of legislation intended to address a wide variety of issues related to individual health insurance. Two important sections of HIPAA include the privacy rules and the security rules. Both of these portions of the law are intended to create safeguards against the unauthorized use, disclosure, or distribution of an individual's health-related information without their specific consent or authorization. While the privacy rules pertain to all Protected Health Information (PHI) including paper and electronic, the security rules deal specifically with Electronic Protected Health Information (EPHI). These rules lay out three types of security safeguards required for compliance: *administrative*, *physical*, and *technical*. For each of these types, the rules identify various security standards, and for each standard, name both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the HIPAA regulation. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications.

Sarbanes-Oxley. The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called Sarbanes-Oxley, Sarbox, or SOX, is a U.S. federal law enacted on July 30, 2002, as a reaction to a number of major corporate and accounting scandals, including those affecting Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom. These scandals, which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets. Named after sponsors U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley, the act was approved by the House by a vote of 334-90 and by the Senate 99-0. President George W. Bush signed it into law, stating it included "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt."

The legislation set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. It does not, however, apply to privately held companies. The act contains 11 sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

Debate continues over the perceived benefits and costs of SOX. Supporters contend the legislation was necessary and has played a useful role in restoring public confidence in the nation's capital markets by, among other things, strengthening corporate accounting controls. Opponents of the bill claim it has reduced America's international competitive edge against foreign financial service providers, saying SOX has introduced an overly complex and regulatory environment into U.S. financial markets.

Computer Libel and Censorship

The opposite side of the privacy debate is the right of people to know about matters others may want to keep private (freedom of information), the right of people to express their opinions about such matters (freedom of speech), and the right of people to publish those opinions (freedom of the press). Some of the biggest battlegrounds in the debate are the bulletin boards, e-mail boxes, and online files of the Internet and public information networks such as America Online and the Microsoft Network. The weapons being used in this battle include *spamming*, *flame mail*, libel laws, and censorship.

Spamming is the indiscriminate sending of unsolicited e-mail messages (*spam*) to many Internet users. Spamming is the favorite tactic of mass mailers of unsolicited advertisements, or *junk e-mail*. Spamming has also been used by cyber-criminals to spread computer viruses or infiltrate many computer systems.

Flaming is the practice of sending extremely critical, derogatory, and often vulgar e-mail messages (*flame mail*) or newsgroup postings to other users on the Internet or online services. Flaming is especially prevalent on some of the Internet's special-interest newsgroups.

There have been many incidents of racist or defamatory messages on the Web that have led to calls for censorship and lawsuits for libel. In addition, the presence of sexually explicit material at many World Wide Web locations has triggered lawsuits and censorship actions by various groups and governments.

The Current State of Cyber Law

Cyber law is the term used to describe laws intended to regulate activities over the Internet or via the use of electronic data communications. Cyber law encompasses a wide variety of legal and political issues related to the Internet and other communications technologies, including intellectual property, privacy, freedom of expression, and jurisdiction.

The intersection of technology and the law is often controversial. Some feel that the Internet should not (or possibly cannot) be regulated in any form. Furthermore, the development of sophisticated technologies, such as encryption and cryptography, make traditional forms of regulation extremely difficult. Finally, the fundamental end-to-end nature of the Internet means that if one mode of communication is regulated or shut down, another method will be devised and spring up in its place. In the words of John Gilmore, founder of the Electronic Frontier Foundation, "the Internet treats censorship as damage and simply routes around it."

One example of advancements in cyber law is found in the Federal Trade Commission's (FTC) Consumer Sentinel Project. Consumer Sentinel is a unique investigative cyber-tool that provides members of the Consumer Sentinel Network with access to data from millions of consumer complaints. Consumer Sentinel includes complaints about identity theft, do-not-call registry violations, computers, the Internet, and online auctions, telemarketing scams, advance-fee loans, and credit scams, sweepstakes, lotteries, and prizes, business opportunities and work-at-home schemes, health and weight loss products, debt collection, credit reports, and other financial matters.

Consumer Sentinel is based on the premise that sharing information can make law enforcement even more effective. To that end, the Consumer Sentinel Network provides law-enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

According to the FTC Sentinel Report for 2007, more than 800,000 complaints were processed through Sentinel with Internet-related offenses representing 11 percent of the total complaints, and computer-related identity theft representing 23 percent. While many of these complaints are difficult, if not impossible to prosecute, we are beginning to see more resources being committed to addressing cyber-related crime.

Cyber law is a new phenomenon, having emerged after the onset of the Internet. As we know, the Internet grew in a relatively unplanned and unregulated manner. Even the early pioneers of the Internet could not have anticipated the scope and

far-reaching consequences of the cyberspace of today and tomorrow. Although major legal disputes related to cyber activities certainly arose in the early 1990s, it was not until 1996 and 1997 that an actual body of law began to emerge. The area, clearly in its infancy, remains largely unsettled. The debate continues regarding the applicability of analogous legal principles derived from prior controversies that had nothing to do with cyberspace. As we progress in our understanding of the complex issues in cyberspace, new and better laws, regulations, and policies will likely be adopted and enacted.

Other Challenges

Let's now explore some other important challenges that arise from the use of information technologies in business, as illustrated in Figure 13.2. These challenges include the potential ethical and societal impact of business applications of IT in the areas of employment, individuality, working conditions, and health.

Employment Challenges

The impact of information technologies on employment is a major ethical concern that is directly related to the use of computers to achieve automation of work activities. There can be no doubt that the use of information technologies has created new jobs and increased productivity while also causing a significant reduction in some types of job opportunities. For example, when computers are used for accounting systems or the automated control of machine tools, they are accomplishing tasks formerly performed by many clerks and machinists. Also, jobs created by information technology may require different types of skills and education than do the jobs that are eliminated. Therefore, people may become unemployed unless they can be retrained for new positions or new responsibilities.

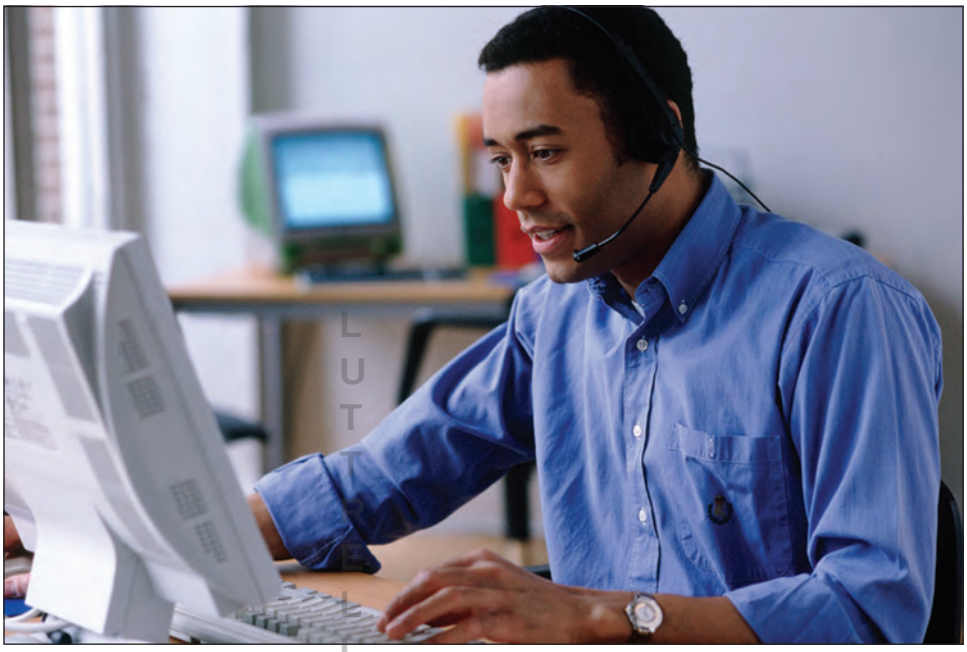
However, there can be no doubt that Internet technologies have created a host of new job opportunities. Many new jobs, including Internet Web masters, e-commerce directors, systems analysts, and user consultants, have been created to support e-business and e-commerce applications. Additional jobs have been created because information technologies make possible the production of complex industrial and technical goods and services that would otherwise be impossible to produce. Thus, jobs have been created by activities that are heavily dependent on information technology, in such areas as space exploration, microelectronic technology, and telecommunications.

Computer Monitoring

One of the most explosive ethical issues concerning workplace privacy and the quality of working conditions in business is **computer monitoring**. That is, computers are being used to monitor the productivity and behavior of millions of employees while they work. Supposedly, computer monitoring occurs so employers can collect productivity data about their employees to increase the efficiency and quality of service. However, computer monitoring has been criticized as unethical because it monitors individuals, not just work, and is done continually, which violates workers' privacy and personal freedom. For example, when you call to make a reservation, an airline reservation agent may be timed on the exact number of seconds he or she took per caller, the time between calls, and the number and length of breaks taken. In addition, your conversation may be monitored. See Figure 13.10.

Computer monitoring has been criticized as an invasion of the privacy of employees because, in many cases, they do not know that they are being monitored or don't know how the information is being used. Critics also say that an employee's right of due process may be harmed by the improper use of collected data to make personnel decisions. Because computer monitoring increases the stress on employees who must work under constant electronic surveillance, it has also been blamed for causing health problems among monitored workers. Finally, computer monitoring has been blamed for robbing workers of the dignity of their work. In its extremes, computer monitoring can create an "electronic sweatshop," in which workers are forced to work at a hectic pace under poor working conditions.

FIGURE 13.10
Computer monitoring can be used to record the productivity and behavior of people while they work.



Source: © LWA-JDC/Corbis.

Political pressure is building to outlaw or regulate computer monitoring in the workplace. For example, public advocacy groups, labor unions, and many legislators are pushing for action at the state and federal level in the United States. The proposed laws would regulate computer monitoring and protect the worker's right to know and right to privacy. In the meantime, lawsuits by monitored workers against employers are increasing. So computer monitoring of workers is one ethical issue in business that won't go away.

Challenges in Working Conditions

Information technology has eliminated monotonous or obnoxious tasks in the office and the factory that formerly had to be performed by people. For example, word processing and desktop publishing make producing office documents a lot easier to do, and robots have taken over repetitive welding and spray painting jobs in the automotive industry. In many instances, this shift allows people to concentrate on more challenging and interesting assignments, upgrades the skill level of the work to be performed, and creates challenging jobs requiring highly developed skills in the computer industry and computer-using organizations. Thus, information technology can be said to upgrade the quality of work because it can upgrade the quality of working conditions and the content of work activities.

Of course, some jobs in information technology—data entry, for example—are quite repetitive and routine. Also, to the extent that computers are used in some types of automation, IT must take some responsibility for the criticism of assembly-line operations that require the continual repetition of elementary tasks, thus forcing a worker to work like a machine instead of like a skilled craftsperson. Many automated operations are also criticized for relegating people to a "do-nothing" standby role, where workers spend most of their time waiting for infrequent opportunities to push some buttons. Such effects do have a detrimental effect on the quality of work, but they must be compared against the less burdensome and more creative jobs created by information technology.

Challenges of Individuality

A frequent criticism of information systems centers on their negative effect on the individuality of people. Computer-based systems are criticized as impersonal systems that dehumanize and depersonalize activities that have been computerized because they eliminate the human relationships present in noncomputer systems.

Another aspect of the loss of individuality is the regimentation that seems required by some computer-based systems. These systems do not appear to possess any flexibility. They demand strict adherence to detailed procedures if the system is to work. The negative impact of IT on individuality is reinforced by horror stories that describe how inflexible and uncaring some organizations with computer-based processes are when it comes to rectifying their own mistakes. Many of us are familiar with stories of how computerized customer billing and accounting systems continued to demand payment and send warning notices to a customer whose account had already been paid, despite repeated attempts by the customer to have the error corrected.

However, many business applications of IT are designed to minimize depersonalization and regimentation. For example, many e-commerce systems stress personalization and community features to encourage repeated visits to e-commerce Web sites. Thus, the widespread use of personal computers and the Internet has dramatically improved the development of people-oriented and personalized information systems.

Health Issues

The use of information technology in the workplace raises a variety of health issues. Heavy use of computers is reportedly causing health problems like job stress, damaged arm and neck muscles, eyestrain, radiation exposure, and even death by computer-caused accidents. For example, computer monitoring is blamed as a major cause of computer-related job stress. Workers, unions, and government officials criticize computer monitoring as putting so much stress on employees that it leads to health problems.

People who sit at PC workstations or visual display terminals (VDTs) in fast-paced, repetitive keystroke jobs can suffer a variety of health problems known collectively as *cumulative trauma disorders* (CTDs). Their fingers, wrists, arms, necks, and backs may become so weak and painful that they cannot work. Strained muscles, back pain, and nerve damage may result. In particular, some computer workers may suffer from *carpal tunnel syndrome*, a painful, crippling ailment of the hand and wrist that typically requires surgery to cure.

Prolonged viewing of video displays causes eyestrain and other health problems in employees who must do this all day. Radiation caused by the cathode ray tubes (CRTs) that produce video displays is another health concern. CRTs produce an electromagnetic field that may cause harmful radiation of employees who work too close for too long in front of video monitors. Some pregnant workers have reported miscarriages and fetal deformities due to prolonged exposure to CRTs at work. Studies have failed to find conclusive evidence concerning this problem; still, several organizations recommend that female workers minimize their use of CRTs during pregnancy.

Ergonomics

Solutions to some of these health problems are based on the science of **ergonomics**, sometimes called *human factors engineering*. See Figure 13.11. The goal of ergonomics is to design healthy work environments that are safe, comfortable, and pleasant for people to work in, thus increasing employee morale and productivity. Ergonomics emphasizes the healthy design of the workplace, workstations, computers and other machines, and even software packages. Other health issues may require ergonomic solutions emphasizing job design rather than workplace design. For example, this approach may require policies providing for work breaks from heavy video monitor use every few hours, while limiting the CRT exposure of pregnant workers. Ergonomic job design can also provide more variety in job tasks for those workers who spend most of their workday at computer workstations.

Societal Solutions

As we noted at the beginning of the chapter, the Internet and other information technologies can have many beneficial effects on society. We can use information technologies to solve human and social problems through **societal solutions** such as medical diagnosis, computer-assisted instruction, governmental program planning, environmental quality control, and law enforcement. For example, computers can help diagnose an illness,

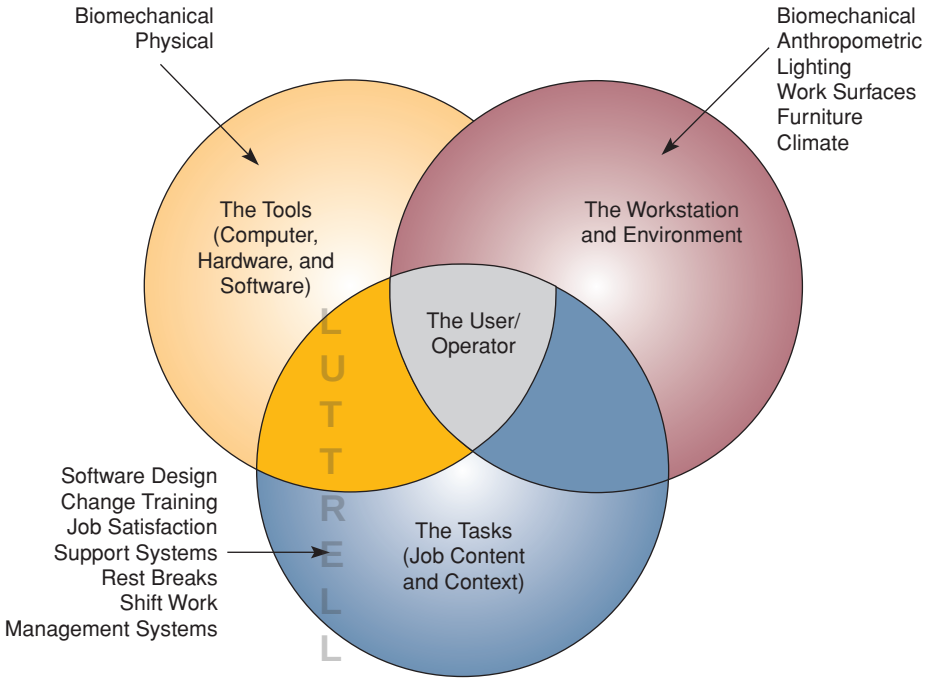


FIGURE 13.11
Ergonomic factors in the workplace. Note that good ergonomic design considers tools, tasks, the workstation, and the environment.

prescribe necessary treatment, and monitor the progress of hospital patients. Computer-assisted instruction (CAI) and computer-based training (CBT) enable interactive instruction tailored to the needs of students. Distance learning is supported by telecommunications networks, videoconferencing, e-mail, and other technologies.

Information technologies can be used for crime control through various law-enforcement applications. For example, computerized alarm systems allow police to identify and respond quickly to evidence of criminal activity. Computers have been used to monitor the level of pollution in the air and in bodies of water, detect the sources of pollution, and issue early warnings when dangerous levels are reached. Computers are also used for the program planning of many government agencies in such areas as urban planning, population density and land use studies, highway planning, and urban transit studies. Computers are being used in job placement systems to help match unemployed persons with available jobs. These and other applications illustrate that information technology can be used to help solve the problems of society.

Obviously, individuals or organizations that do not accept ethical responsibility for their actions cause many of the detrimental effects of information technology. Like other powerful technologies, information technology possesses the potential for great harm or great good for all humankind. If managers, business professionals, and IS specialists accept their ethical responsibilities, then information technology can help improve living and working conditions for all of society.

SECTION II Security Management of Information Technology

Introduction

With Internet access proliferating rapidly, one might think that the biggest obstacle to e-commerce would be bandwidth. But it's not; the number one problem is security. And part of the problem is that the Internet was developed for interoperability, not impenetrability.

As we saw in Section I, there are many significant threats to the security of information systems in business. That's why this section is dedicated to exploring the methods that companies can use to manage their security. Business managers and professionals alike are responsible for the security, quality, and performance of the business information systems in their business units. Like any other vital business assets, hardware, software, networks, and data resources need to be protected by a variety of security measures to ensure their quality and beneficial use. That's the business value of security management.

Read the Real World Case on the next page. We can learn a lot about why IT managers are increasingly concerned about securing the user end of their networks, and how they are facing this challenge. See Figure 13.12.

Tools of Security Management

The goal of **security management** is the accuracy, integrity, and safety of all information system processes and resources. Thus, effective security management can minimize errors, fraud, and losses in the information systems that interconnect today's companies and their customers, suppliers, and other stakeholders. As Figure 13.13 illustrates, security management is a complex task. As you can see, security managers must acquire and integrate a variety of security tools and methods to protect a company's information system resources. We discuss many of these security measures in this section.

Top Executives Agree: Information Security Is a Top Priority

What do chief executive officers and other business leaders really think about information security? A recent survey and interviews conducted by *InformationWeek* reveal that they're more aligned with "infosec" (information security) teams than you might think—when comes to information security, non-IT executives just might get it. The results suggest that C-level executives not only recognize the importance of information security, but actively support the efforts of their IT organizations to protect corporate assets and reduce risk.

At times, that comes as a surprise. The rants from IT pros about stingy executives who are ignorant of critical security issues and regard security as an impediment to doing business are quite common. Indeed, conflicts between executives and IT organizations are still common. Moneymaking opportunities that present considerable security risks still go forward over the objections of information security teams. Conversely, security teams don't always appreciate that risk can't be entirely eliminated, or that some security measures go so far as to make information and technology too cumbersome to be useful.

Among the more security-minded executives is William McNabb, chief executive officer of investment firm Vanguard Group. He sums up his company's information security responsibility this way: "We manage more than a trillion dollars of other people's money. That's important trust they've placed with us, and we have to do everything in our power to protect it." Seventy-five percent of survey respondents say information security is among the highest of corporate priorities.

There are four major reasons for this high level of executive support. First is the rise of high-volume theft of credit card information, Social Security numbers, and other personal data. Such attacks began to make headlines in 2005, when DSW Shoe Warehouse and ChoicePoint were hit. In the DSW case, thieves stole 1.4 million

(text continues on page 558)

REAL WORLD CASE 2

Wyoming Medical Center, Los Angeles County, and Raymond James: End-Point Security Gets Complicated

Users say protecting network end points is becoming more difficult as the type of endpoint devices—desktops, laptops, smartphones—grows, making security a complex moving target. The problem is compounded by the range of what groups within corporations do on these devices, which translates into different levels of protection for classes of users on myriad devices.

"Deciding the appropriate device defense becomes the No. 1 job of endpoint security specialists," says Jennifer Jabbush, CISO of Carolina Advanced Digital consultancy. Depending on the device and the user's role, end points need to be locked down to a greater or lesser degree.

For instance, Wyoming Medical Center in Casper, Wyoming, has four classifications of PCs: "open PCs in hallways for staff use; PCs at nursing stations; PCs in offices; and PCs on wheels that move between patient rooms and handle very specific, limited applications," says Rob Pettigrew, manager of technical systems and help desk for the center.

Pettigrew is deploying Novell ZenWorks to 850 of the center's 900 PCs in order to make sure each class has the right software. With 110 applications and 40 major medical software systems, that makes a huge matrix of machine types and restrictions to contend with, he says.

In addition, physicians in affiliated clinics can access via SSL VPN (a kind of VPN that is accessible over Web browsers), but they are limited to reaching Web servers in a physician's portal, which is protected from the hospital data network. Some Citrix thin clients are also used to protect data from leaving the network but overall the strategy for unmanaged machines is a work in progress, Pettigrew says. "We're hoping to get more help desk to deal with the external physicians," he says.

One concern that can be addressed by endpoint security is data privacy, which is paramount for the Los Angeles County Department of Health Services in California, says Don Zimmer, information security officer for the department. He supports about 18,000 desktops and laptops and operates under the restrictions of Health Insurance Portability and Accountability Act (HIPAA) regulations. "That means disk encryption," he says.

"If it's not encrypted and there is a breach, then we have to start calling people," he says. To avoid violating patients' privacy and a loss of public trust, the department encrypts the drives of all the PC end points with software from PointSec.

Equally important is keeping sensitive information off movable media that can plug into USB ports. The department uses Safend's USB Port Protector product that either denies access to sensitive documents or requires that they be encrypted and password-protected before being placed on the removable device.

Everyone's talking about the insider threat. But protecting data can't supersede the requirement to give users the access they need to do their jobs—otherwise, soon you'll have neither business data nor employees to worry about.

Striking a balance between access and protection isn't easy, however. In an *InformationWeek* Analytics/DarkReading.com endpoint security survey of 384 business technology pros, 43 percent classify their organizations as "trusting," allowing data to be copied to USB drives or other devices with no restrictions or protective measures.

Still, IT is aware of the need to move from a stance of securing end points to assuming that laptops and smartphones will be lost, good employees will go bad, and virtual machines will be compromised. Instead of focusing on end points, let fortifications follow the data: Decide what must be protected, find out everywhere it lives, and lock it down against both inside and outside threats, whether via encryption, multitiered security suites, or new technologies like data loss prevention (DLP).

DLP suites combine network scanning and host-based tools to collect, categorize, and protect corporate intellectual property. These products can maintain an archive of data and documents, along with associated permissions by group, individual, and other policies.

They then actively scan internal networks and external connections looking for anomalies. This takes data protection beyond perimeter or endpoint protection; DLP facilitates internal safety checks, allowing "eyes-only" data to remain eyes only and minimizing the risk that sensitive data will be viewed by the wrong folks, even in-house.

Zimmer says he is looking into DLP software as well that can restrict the access individual devices have to data.

FIGURE 13.12

The proliferation of end-user devices is making endpoint security more important than ever.

Source: © Bloomberg/Getty Images.

Although the technology can be effective, it also requires that businesses locate and classify their data so they can set policies surrounding it—a job that can seem insurmountable, depending on how data have been stored.

For Pettigrew, this means finding the 5 percent of sensitive data stored outside the medical center's electronic medical records system.

Rather than deal with many vendors for specific endpoint protection products, some businesses opt for endpoint security suites, such as those that evolved from the antivirus roots of vendors, including McAfee and Symantec.

Sam Ghelfi, chief security officer at financial firm Raymond James, opted for Sophos's Endpoint Protection and Data Security Suite, which offers firewall, antivirus, data loss prevention, antispyware, encryption, and network access control (NAC). The company wants tight control over the Web content that is available to users to minimize the malware coming in via basic Web browsing. The company uses a Sophos Web proxy that filters sites based on reputation, but also the content that sites return.

Mobile devices that could contain confidential company information are disk encrypted, again using Sophos agents. If a device is lost or stolen, the encryption key is wiped out, making it impossible to decrypt the contents of the hard drive.

Ghelfi says he believes in personal firewalls on individual machines because they can stop groups of devices from talking to other groups. "Centrally managed, they can reveal network traffic patterns," he says.

He doesn't use all of the features of the Sophos suite, though. For instance, he is just getting around to implementing NAC to let unmanaged guest machines get on the network but still minimize risk that they are infected.

That will clear them based on authentication, access method and type of machine, but for contractors that require access to the main network, he also insists that they install the Sophos suite. Other unmanaged machines, such as those of guests, are allowed access only through a dedicated wireless network that leads to a limited set of servers in a network segment flanked by firewalls, he says.

"Such endpoint security suites can be attractive financially," Jabbusch says, "because customers can wind up with reduced agent, license and support fees and less management overhead." There may be a certain amount of convenience if customers decide to layer on more applications within a suite.

The newest class of devices—smartphones—is presenting ongoing challenges as organizations figure out how to deal with them. Particularly dicey is whether to allow employees to use their personally owned devices for business and to access the business network.

The jury is still out, at least among state government chief information officers. A recent survey by the National Association of State Chief Information Officers says that of 36 states responding to a survey, 39 percent say they allow personal smartphones if they are protected by state security measures. Twenty-seven percent say they don't allow personal smartphones on their networks, 17 percent say they are reviewing state policy, and 17 percent say they don't have statewide control—each agency sets its own policies.

A separate Forrester Research survey says that 73 percent of businesses surveyed are at least somewhat concerned about smartphones being authorized for business use. According to DeviceLock, its survey of more than 1000 IT professionals found that fewer than 40 percent of respondents said yes to the question: "Have you taken any steps to secure your business against the security threat posed by iPhones? "Analyzing the responses by region, researchers found that only 25 percent of respondents in North America and Western Europe said yes to the question, suggesting this is a "back burner" security issue, says the endpoint data leak-prevention specialist.

Jabbush says the type of smartphone is a factor. "I can't imagine allowing an iPhone," she says. "A BlackBerry is somewhat better" because BlackBerries have a management infrastructure and the devices can be locked down to corporate policies.

Mobile device security is one of those areas that should get more attention. However, it is likely that this topic will remain buried—until a lost or stolen iPhone leads to a visible and costly security breach.

Source: Adapted from Tim Greene, "Endpoint Security Gets Complicated," *Network World*, April 1, 2010; and Joe Hernick, "InformationWeek Analytics: Endpoint Security and DLP," *InformationWeek*, April 27, 2009.

LUTTRELL, SONYA LOUISE 256 6BU

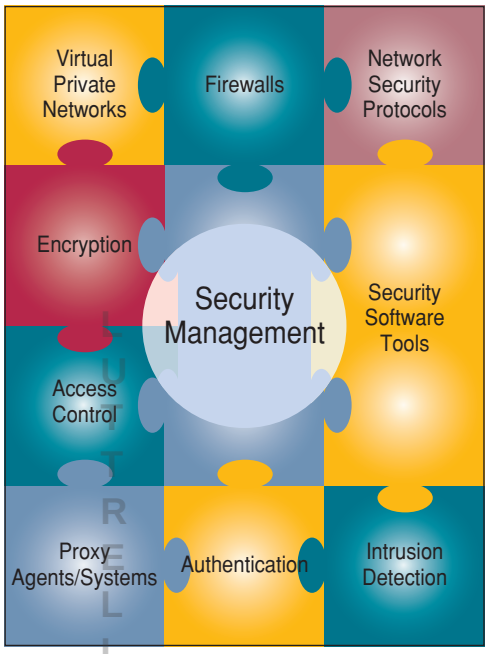
CASE STUDY QUESTIONS

1. What is the underlying issue behind endpoint security, and why is it becoming even more difficult for companies to address it? Define the problem in your own words using examples from the case.
2. What are the different approaches taken by the organizations in the case to address this issue? What are the advantages and disadvantages of each? Provide at least two examples for each alternative.
3. A majority of respondents to a survey discussed in the case described their company as "trusting." What does this mean? What is the upside of a company being "trusting"? What is the downside? Provide some examples to illustrate your answers.

REAL WORLD ACTIVITIES

1. Data loss prevention (DLP) was a technology mentioned in the case, and one that is garnering more and more attention from corporate security departments. Go online and research what DLP involves, and look for examples of its application to actual problems, and their outcomes. Prepare a report to summarize your work.
2. Whether to allow employees to use their own smartphones (or other devices yet to be invented) on corporate networks is quickly becoming a contested issue. What do companies stand to gain, or lose, in either case? What about employees? Break into small groups with your classmates to discuss these questions.

FIGURE 13.13
Examples of important security measures that are part of the security management of information systems.



Source: Courtesy of Wang Global.

credit card numbers from stores in 25 states. Meanwhile, poor controls at ChoicePoint enabled scam artists posing as legitimate businesses to access consumer records and perpetrate identity theft. Since then, a string of larger information thefts from the likes of the Hannaford Bros, grocery chain, job site Monster.com, retailer TJX, and, most recently, Heartland Payment systems has put executives on notice: Such breaches can no longer be dismissed as merely isolated incidents.

Second, the high-profile thefts have triggered a number of state breach-disclosure laws, which compel companies to publicize the theft or loss of personally identifiable information. Companies also face industry data-protection standards, the most prominent of which is the Payment Card Industry Data Security Standard, which requires a variety of security measures for businesses that accept and process credit cards.

The third trend changing executives' attitudes about security is the rising cost of information breaches.

From lawsuit payouts to fines to the expense of setting up credit-monitoring services for victimized customers, executives can see exactly how much a security failure costs. U.S. companies paid an average of $202 per exposed record in 2008, up from $197 in 2007, according to a report by the Ponemon Institute, a privacy management researcher. The report also says the average total cost per breach for each company was $6.6 million in 2008, up from $6.3 million in 2007 and $4.7 million in 2006.

The fourth major trend is the damage to a company's brand and reputation. While it's hard to put a price on the loss of customer trust or efforts to repair a brand, no CEO wants to have to try to do that math.

Source: Adapted from Andrew Conry-Murray, "A Unified Front," *InformationWeek*, February 16, 2009.

Inter-Networked Security Defenses

Few professionals today face greater challenges than those IT managers who are developing Internet security policies for rapidly changing network infrastructures. How can they balance the need for Internet security and Internet access? Are the budgets for Internet security adequate? What impact will intranet, extranet, and Web application development have on security architectures? How can they come up with best practices for developing Internet security policy?

The security of today's networked business enterprises is a major management challenge. Many companies are still in the process of getting fully connected to the Web and the Internet for e-commerce and are reengineering their internal business processes with intranets, e-business software, and extranet links to customers, suppliers, and other business partners. Vital network links and business flows need to be protected from external attack by cyber-criminals and from subversion by the criminal or irresponsible acts of insiders. This protection requires a variety of security tools and defensive measures and a coordinated security management program. Let's take a look at some of these important security defenses.

Encryption

Encryption of data has become an important way to protect data and other computer network resources, especially on the Internet, intranets, and extranets. Passwords, messages, files, and other data can be transmitted in scrambled form and unscrambled by computer systems for authorized users only. Encryption involves using special mathematical algorithms, or keys, to transform digital data into a scrambled code before they are transmitted, and then to decode the data when they are received. The most widely used encryption method uses a pair of public and private keys unique to each individual. For example, e-mail could be scrambled and encoded using a unique *public key* for the recipient that is known to the sender. After the e-mail is transmitted, only the recipient's secret *private key* could unscramble the message. See Figure 13.14.

Encryption programs are sold as separate products or built into other software used for the encryption process. There are several competing software encryption standards, but the top two are RSA (by RSA Data Security) and PGP (which stands for "pretty good privacy"), a popular encryption program available on the Internet. Software products including Microsoft Windows XP, Novell NetWare, and Lotus Notes offer encryption features using RSA software.

FIGURE 13.14 How public key/private key encryption works.

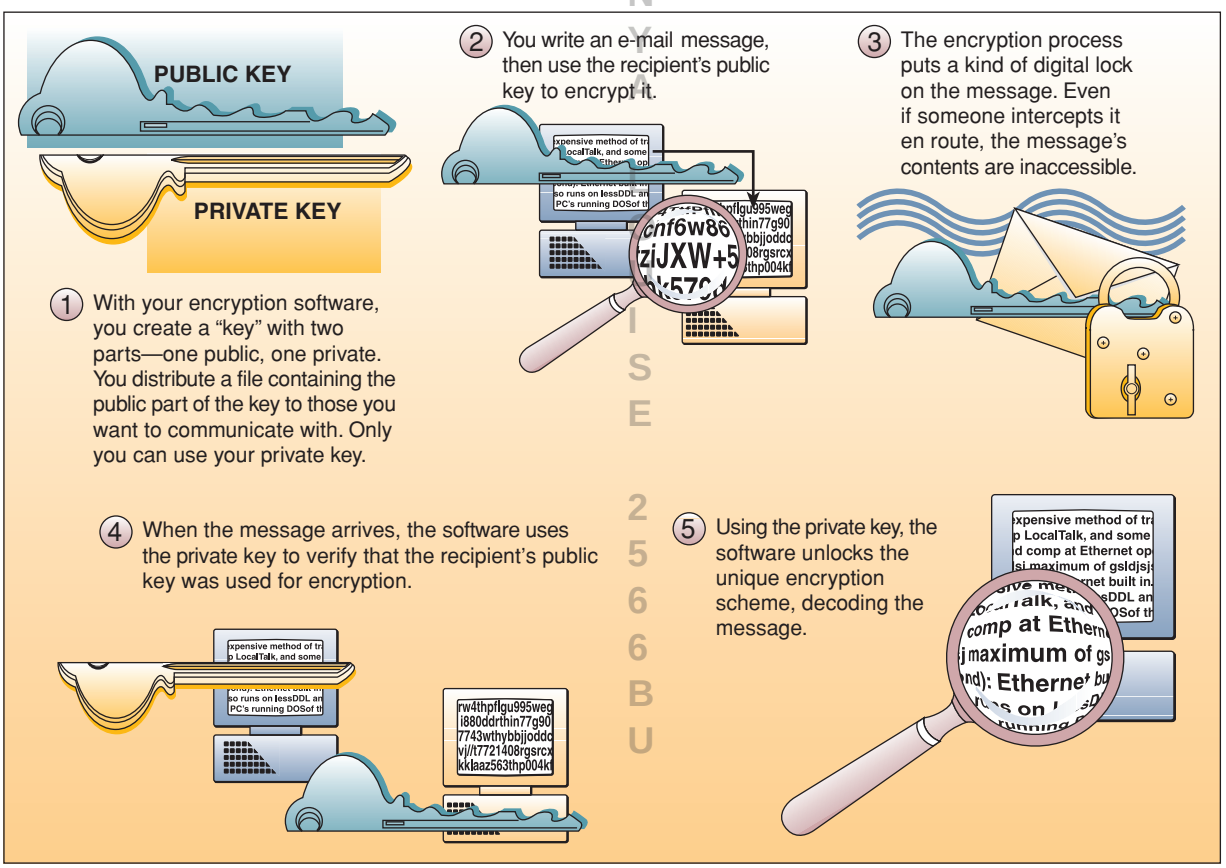
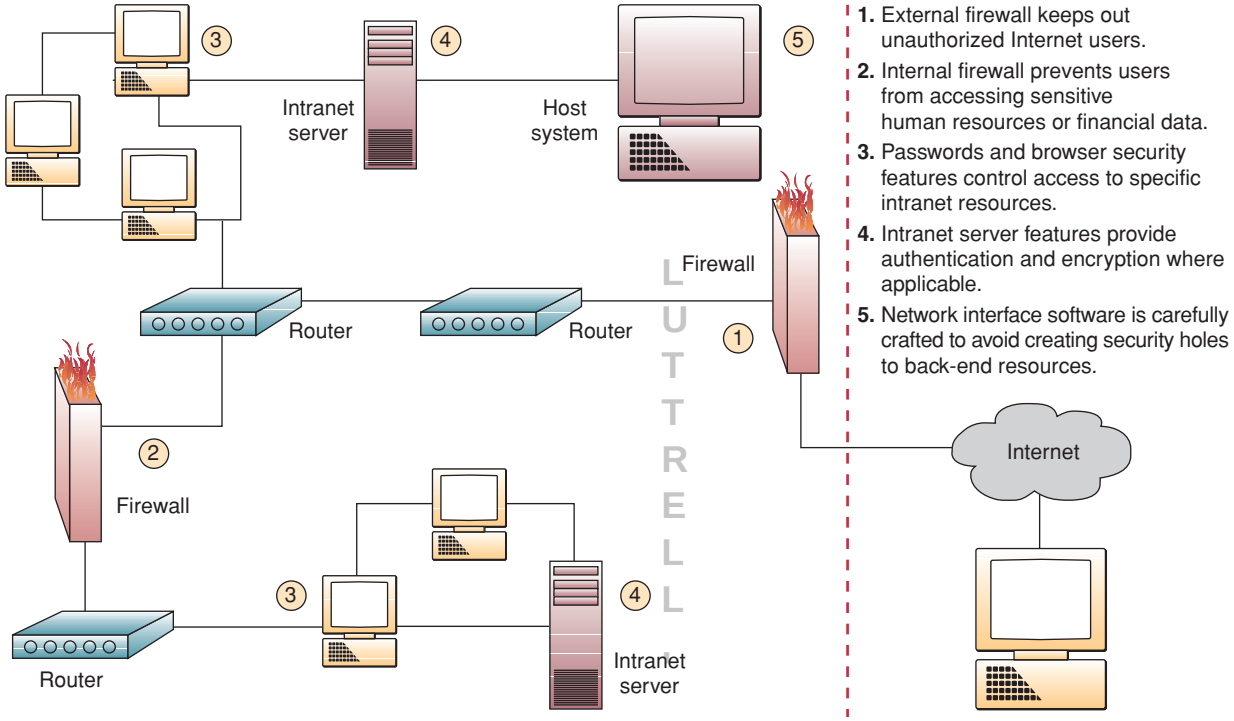


FIGURE 13.15 An example of the Internet and intranet firewalls in a company's networks.



Firewalls

Another important method for control and security on the Internet and other networks is the use of **firewall** computers and software. A network firewall can be a communications processor, typically a *router*, or a dedicated server, along with firewall software. A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and only allows authorized transmissions in and out of the network. Firewall software has also become an essential computer system component for individuals connecting to the Internet with DSL or cable modems because of their vulnerable, "always-on" connection status. Figure 13.15 illustrates an Internet/intranet firewall system for a company.

Firewalls can deter, but not completely prevent, unauthorized access (hacking) into computer networks. In some cases, a firewall may allow access only from trusted locations on the Internet to particular computers inside the firewall, or it may allow only "safe" information to pass. For example, a firewall may permit users to read e-mail from remote locations but not run certain programs. In other cases, it is impossible to distinguish the safe use of a particular network service from unsafe use, so all requests must be blocked. The firewall may then provide substitutes for some network services (such as e-mail or file transfers) that perform most of the same functions but are not as vulnerable to penetration.

WhiteHat Security: "Black Box Testing" Mimics Hackers to Discover Vulnerabilities

Jeremiah Grossman wants you to know that firewalls and SSL encryption won't prevent a hacker from breaking into your e-commerce Web site, compromising your customers' data, and possibly stealing your money. That's because most Web site attacks these days exploit bugs in the Web application itself, rather than in the operating system on which the application is running.

Grossman is the founder and chief technology officer of WhiteHat Security, a Silicon Valley firm that offers an outsourced Web site vulnerability management service. Using a combination of proprietary scanning and so-called ethical hacking, WhiteHat assesses the security of its clients' Web sites, looking for exploitable vulnerabilities.

WhiteHat does its scanning without access to the client's source code and from outside the client's firewall using the standard HTTP Web protocol. This approach is sometimes called "black box testing" because the Web site's contents are opaque to the security assessors. The problem with black box testing, of course, is that it is sure to miss many vulnerabilities and back doors that are hidden in the source code. Black box testing can only find vulnerabilities that are visible to someone who is using your Web site, but the advantage of this approach is that it precisely mimics how a hacker would most likely conduct his reconnaissance and break-in.

From his vantage point at WhiteHat, Grossman has seen several organizations migrate Web sites from Microsoft's original ASP to ASP.NET. "ASP classic, the first generation of ASP websites, are generally riddled with vulnerabilities," he says. Yet when these organizations rewrote their applications using ASP.NET, suddenly their applications improved tremendously security-wise. "Same developers, two different frameworks. It wasn't an education problem; it was a technology problem."

At another company—a financial institution—WhiteHat discovered an easily exploited vulnerability that would have let customers steal money. WhiteHat called up the company, and the problem was hot-fixed within 24 hours. A few months later, the vulnerability came back. "The developers were working on the next release, set to come out in two to three months. Some developer did not back-port the hot-fix from the production server to the development server. So when the push occurred three months later, they pushed the vulnerability again." Ugh!

You may not be a big fan of this approach to security, but if you talk to Grossman for a couple of hours, he will convince you that it's a necessary part of today's e-commerce Web sites. Yes, it would be nice to eliminate these well-known bugs with better coding practices, but we live in the real world. It's better to look for the bugs and fix them than to just cross your fingers and hope that they aren't there.

Source: Adapted from Simson Garfinkel, "An Introduction to the Murky Science of Web Application Security," *CIO Magazine*, May 11, 2007.

Denial of Service Attacks

Major attacks against e-commerce and corporate Web sites in the past few years have demonstrated that the Internet is extremely vulnerable to a variety of assaults by criminal hackers, especially **distributed denial of service (DDOS)** attacks. Figure 13.16 outlines the steps organizations can take to protect themselves from DDOS attacks.

Denial of service assaults via the Internet depend on three layers of networked computer systems: (1) the victim's Web site, (2) the victim's Internet service provider (ISP), and (3) the sites of "zombie" or slave computers that the cyber-criminals commandeered. For example, in early 2000, hackers broke into hundreds of servers, mostly poorly protected servers at universities, and planted Trojan horse.exe programs, which were then used to launch a barrage of service requests in a concerted attack on e-commerce Web sites like Yahoo! and eBay.

As Figure 13.16 shows, defensive measures and security precautions must be taken at all three levels of the computer networks involved. These are the basic steps

FIGURE 13.16

How to defend against denial of service attacks.

Defending against Denial of Service
• **At the zombie machines:** Set and enforce security policies. Scan regularly for Trojan horse programs and vulnerabilities. Close unused ports. Remind users not to open .exe mail attachments.
• **At the ISP:** Monitor and block traffic spikes. Filter spoofed IP addresses. Coordinate security with network providers.
• **At the victim's Web site:** Create backup servers and network connections. Limit connections to each server. Install multiple intrusion-detection systems and multiple routers for incoming traffic to reduce choke points.

companies and other organizations can take to protect their Web sites from denial of service and other hacking attacks. Now let's take a look at a real-world example of a more sophisticated defense technology.

As If Phishing Wasn't Enough: Denial of Service Attacks

Kevin Dougherty has seen his share of spam and phishing scams, as has any IT leader in the financial services industry. But the sender's name on this particular e-mail sent a shudder down his spine: It was from one of his board members at the Central Florida Educators' Federal Credit Union (CFEFCU). The e-mail claimed in convincing detail that there was a problem with the migration to a new Visa credit card that the board member was promoting to the credit union's customers. The fraudulent message urged customers to click on a link—to a phony Web site set up by criminals—and enter their account information to fix the problem.

But what happened later that Friday afternoon—after Dougherty, who is senior vice president of IT and marketing, had wiped the credit card migration information off the Web site and put up an alert warning customers of the scam—really scared him.

Around 2 p.m., the site suddenly went dark, like someone had hit it with a baseball bat. That's when Dougherty realized that he was dealing with something he hadn't seen before. And he couldn't describe it with conventional terms like phishing or spamming. This was an organized criminal conspiracy targeting his bank. "This wasn't random," he says. "They saw what we were doing with the credit card and came at us hard."

Dougherty's Web site lay in a coma from a devastating distributed denial of service (DDOS) attack that, at its peak, shot more than 600,000 packets per second of bogus service requests at his servers from a coordinated firing squad of compromised computers around the globe. That the criminals had the skill and foresight to launch a two-pronged attack against Dougherty and his customers was a clear indication of how far online crime, which is now a $2.8 billion business according to research company Gartner, has come in the past few years.

Obviously, the first thing Dougherty had to do was stop the attack. He had to hurriedly assemble a coalition of vendors and consultants to help him, and then he had to convince his CEO that drastic steps were needed—steps that would temporarily cut off customers from any possibility of getting to their accounts online until the problems were completely eradicated. Dougherty wanted to have the site temporarily blacklisted with his telecom provider, BellSouth, to deflect the attack, thereby reducing pressure on the site and giving him the time and flexibility to make protective changes. But his CEO resisted—as might anyone who has not experienced an attack. "He wanted to keep it up so we could service the members," says Dougherty.

At 11 p.m., after a long night of battling the attackers and plotting strategy, Dougherty finally convinced his CEO to have the site blacklisted and to take a break until morning.

Continuing in a tired and emotional state would have played into the attackers' hands. "It's a mind game," says Dougherty.

By Saturday morning, Dougherty had RSA, a security vendor he called in when the attacks began, working to set up a "takedown" service that seeks out and dispatches criminal Web sites (in this case, more than 30) with its own cyber baseball bat. Meanwhile, BellSouth began beefing up security around the credit union site to try to thwart attacks.

The site was back up by Saturday evening. In the end, 22 customers gave up their information to the thieves and the total losses were "less than five figures," says Dougherty. Though the credit union had averted disaster, "it was a rude awakening," he says.

Source: Adapted from Nancy Weil, "Your Plan to Fight Cyber Crime," *CIO Magazine*, June 15, 2007.

E-mail Monitoring

Spot checks just aren't good enough anymore. The tide is turning toward systematic monitoring of corporate e-mail traffic using content-monitoring software that scans for troublesome words that might compromise corporate security. The reason: Users of monitoring software said they're concerned about protecting their intellectual property and guarding themselves against litigation.

As we mentioned in Section I, Internet and other online e-mail systems are one of the favorite avenues of attack by hackers for spreading computer viruses or breaking into networked computers. E-mail is also the battleground for attempts by companies to enforce policies against illegal, personal, or damaging messages by employees versus the demands of some employees and others who see such policies as violations of privacy rights.

Employee Monitoring: Who's Watching Now?

Just the mention of employee monitoring raises concerns about Big Brother and privacy, as well as issues of trust, loyalty, and respect. Yet monitoring employee use of e-mail, the Internet, and telephones in the workplace has become more common than gatherings at the office watercooler. Ten years ago, employee monitoring meant that the supervisor would walk the floor and watch the activities of workers. Today, businesses increasingly use automated tools to ensure that workers are completing tasks, not wasting resources, and complying with a growing list of government regulations.

A report by the Privacy Rights Clearinghouse says there's little that employees can do to limit monitoring by their employers. Bosses have the right to listen to workers' phone calls in most instances, obtain records of those calls, use software to see what's being displayed on computer screens, check what information is stored on hard disks, and track and record e-mail. Some companies have little choice but to monitor employees.

Presidio Financial Partners provides investment consulting services, controlling approximately $3 billion in assets for 150 clients. It falls under the scrutiny of the Securities and Exchange Commission and the National Association of Securities Dealers, and it must provide regulators with access to e-mail and other correspondence between the company and its clients, as well as maintain an archive of the information.

"We have to have this information at our disposal," says Jeff Zlot, managing director for Presidio. "But our clients are high-profile individuals, and the last thing we need is information getting into the wrong hands."

Presidio began to use Fortiva Supervision software from Fortiva to monitor, track, and archive the e-mail of its consultants, and it was pleased that Fortiva keeps archived material encrypted. Fortiva Supervision is used to track e-mail between Presidio salespeople and clients, specifically looking for keywords that could pose problems. "We can show the regulators that we set up guidelines and that we are enforcing those guidelines from a sales supervision standpoint," Zlot says.

Phrases that will be flagged by the software include such things as guaranteed return or guaranteed performance, or any time the word *complaint* is used. If the keywords are spotted, supervisors must review the e-mail. As many as 50 e-mails a day get queued for review. "This forces the sales supervisors to look and approve the work the employees are doing," Zlot says.

The growing number of automated monitoring tools makes it easier for employers to keep an eye on what employees are doing than in the old days—when you really had to keep an eye on them.

Source: Adapted from Darrell Dunn, "Who's Watching Now?" *InformationWeek*, February 27, 2006.

Virus Defenses

Is your PC protected from the latest viruses, worms, Trojan horses, and other malicious programs that can wreak havoc on your PC? Chances are it is, if it's periodically linked to the corporate network. These days, corporate antivirus protection is a centralized function of information technology. Someone installs it for you on your PC and notebook or, increasingly, distributes it over the network. The antivirus software runs in the background, popping up every so often to reassure you. The trend right now is to automate the process entirely.

FIGURE 13.17
An example of security suite PC software that includes antivirus and firewall protection.

Source: Courtesy of McAfee.

Many companies are building defenses against the spread of viruses by centralizing the distribution and updating of **antivirus software** as a responsibility of their IS departments. Other companies are outsourcing the virus protection responsibility to their Internet service providers or telecommunications or security management companies.

One reason for this trend is that the major antivirus software companies like McAfee (VirusScan) and Symantec (Norton Antivirus) have developed network versions of their programs, which they are marketing to ISPs and others as a service they should offer to all their customers. The antivirus companies are also marketing *security suites* of software that integrate virus protection with firewalls, Web security, and content-blocking features. See Figure 13.17.

The Future of Antivirus

Antivirus software makes Greg Shipley so mad he has to laugh. "The relationship between signature-based antivirus companies and the virus writers is almost comical. One releases something and then the other reacts, and they go back and forth. It's a silly little arms race that has no end."

Shipley, chief technology officer at Neohapsis, a security consulting firm in Chicago, says the worst part is that the arms race isn't helpful either to him or to his clients. "I want to get off of signature-based antivirus as rapidly as possible. I think it's a broken model, and I think it's an incredible CPU hog."

Antivirus as an industry has modeled itself on the human immune system, which slaps a label on things like viruses so it knows to attack them when it sees that same label, or signature, again. Signature-based antivirus has moved well beyond that simple type of signature usage (although, at the beginning, it did look for specific lines of code). The number of malware signatures that security software company F-Secure tracked doubled in 2007, and while you might cynically expect such a company to say there's more malware out there, 2007's total doubled the number of signatures F-Secure had built up over the previous 20 years.

Antivirus firms think that reports of their death are greatly exaggerated, thank you very much—even those that aren't overly reliant on signatures, like BitDefender, which says that signature-based techniques account for only 20 percent of the malware it catches. Corporate CISOs (chief information security officers) certainly don't expect to find one answer to their problems. "If you rely on signatures for security, you're pretty much dead in the water," says Ken Pfeil, head of information security for the Americas region of WestLB, a German bank. Pfeil thinks signatures are useful and his firm uses them, but when new malware appears, he often finds it faster to try to break it down himself to understand its potential effects, rather than wait for his vendor to give him an update. His firm has also adopted tools that use heuristics techniques and anomaly testing, to add oomph to its antivirus approach.

That kind of layered approach to software fits with where Natalie Lambert, an analyst at Forrester Research, thinks the market is going. "Signature-based antivirus plus techniques like heuristic information processing systems, or HIPS, which look for suspicious actions by software, like an application opening itself from the Temp folder." The downside to these technologies is that none is as simple and alluring as the old signature-based antivirus, which she called a "set it and forget it" technology. She notes that HIPS technologies are difficult to manage and will never be as simple as the old model, although she expects they will get easier over time.

Antivirus firms agree that they are becoming something different; however, David Harley, administrator of Avien, the antivirus information exchange network, thinks that there are psychological reasons that antivirus software is unlikely to go away. "The idea of a solution that stops real threats and doesn't hamper nonmalicious objects and processes is very attractive. People (at any rate, those who aren't security specialists) like the idea of threat-specific software, as long it catches all incoming malware and doesn't generate any false positives, because then they can just install it and forget about it. Unfortunately, that's an unattainable ideal."

Note to Greg Shipley: Don't hold your breath on getting rid of your antivirus software.

Source: Adapted from Michael Fitzgerald, "The Future of Antivirus," *Computerworld*, April 14, 2008.

Other Security Measures

Let's now briefly examine a variety of security measures that are commonly used to protect business systems and networks. These include both hardware and software tools, like fault-tolerant computers and security monitors, and security policies and procedures, like passwords and backup files. All are part of an integrated security management effort at many companies today.

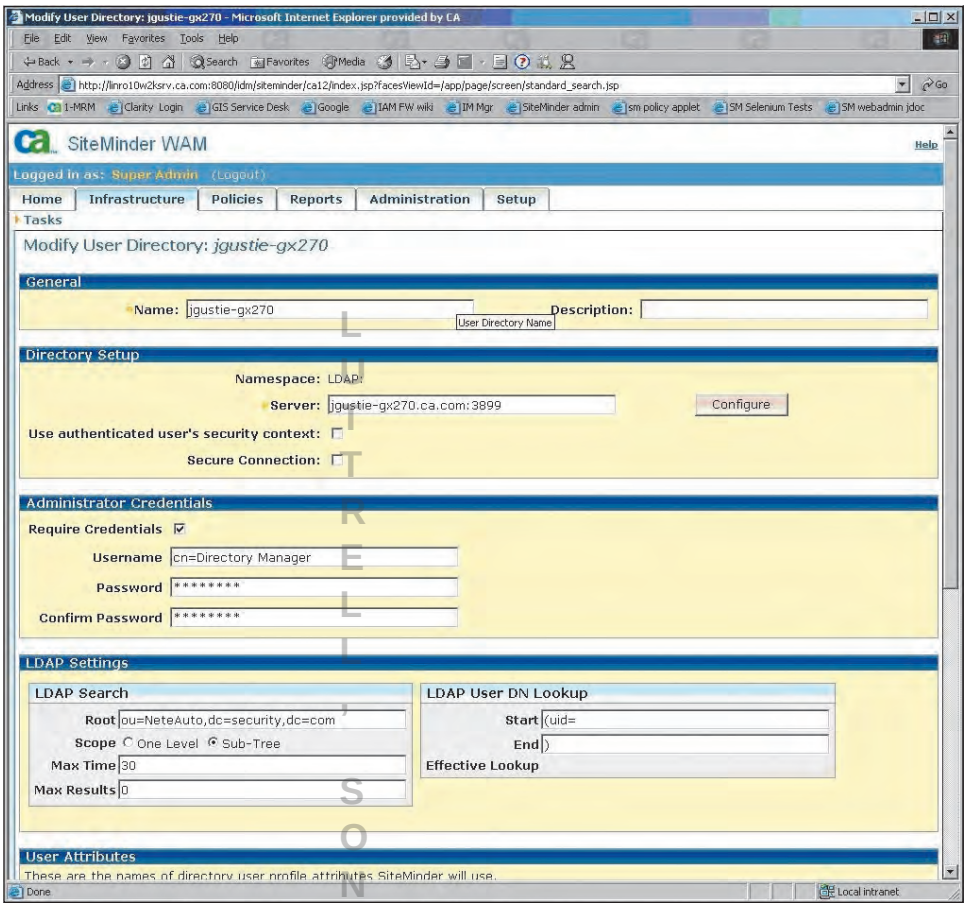
Security Codes

Typically, a multilevel **password** system is used for security management. First, an end user logs on to the computer system by entering his or her unique identification code, or user ID. Second, the end user is asked to enter a password to gain access into the system. (Passwords should be changed frequently and consist of unusual combinations of upper- and lowercase letters and numbers.) Third, to access an individual file, a unique file name must be entered. In some systems, the password to read the contents of a file is different from that required to write to a file (change its contents). This feature adds another level of protection to stored data resources. For even stricter security, however, passwords can be scrambled, or *encrypted*, to avoid their theft or improper use, as we will discuss shortly. In addition, *smart cards*, which contain microprocessors that generate random numbers to add to an end user's password, are used in some secure systems.

Backup Files

Backup files, which are duplicate files of data or programs, are another important security measure. Files can also be protected by *file retention* measures that involve storing copies of files from previous periods. If current files are destroyed, the files from previous

FIGURE 13.18
The eTrust security monitor manages a variety of security functions for major corporate networks, including monitoring the status of Web-based applications throughout a network.



Source: Courtesy of Site Minder.

periods can be used to reconstruct new current files. Sometimes, several generations of files are kept for control purposes. Thus, master files from several recent periods of processing (known as *child*, *parent*, and *grandparent* files) may be kept for backup purposes. Such files may be stored off-premises, that is, in a location away from a company's data center, sometimes in special storage vaults in remote locations.

Security Monitors

Security of a network may be provided by specialized system software packages known as **system security monitors**. See Figure 13.18. System security monitors are programs that monitor the use of computer systems and networks and protect them from unauthorized use, fraud, and destruction. Such programs provide the security measures needed to allow only authorized users to access the networks. For example, identification codes and passwords are frequently used for this purpose. Security monitors also control the use of the hardware, software, and data resources of a computer system. For example, even authorized users may be restricted to the use of certain devices, programs, and data files. In addition, security programs monitor the use of computer networks and collect statistics on any attempts at improper use. They then produce reports to assist in maintaining the security of the network.

Biometric Security

Biometric security is a fast-growing area of computer security. These are security measures provided by computer devices that measure physical traits that make each individual unique, such as voice verification, fingerprints, hand geometry, signature dynamics, keystroke analysis, retina scanning, face recognition, and genetic pattern analysis. Biometric control devices use special-purpose sensors to measure and digitize a biometric profile of a person's fingerprints, voice, or other physical trait. The digitized signal is processed and compared to a previously processed profile of the individual stored on

FIGURE 13.19
An evaluation of common biometric security techniques based on user requirements, accuracy, and cost.

Evaluation of Biometric Techniques

	User Criteria		System Criteria	
	Intrusiveness	Effort	Accuracy	Cost
Dynamic signature verification	Excellent	Fair	Fair	Excellent
Face geometry	Good	Good	Fair	Good
Finger scan	Fair	Good	Good	Good
Hand geometry	Fair	Good	Fair	Fair
Passive iris scan	Poor	Excellent	Excellent	Poor
Retina scan	Poor	Poor	Very good	Fair
Voice print	Very good	Poor	Fair	Very good

magnetic disk. If the profiles match, the individual is allowed entry into a computer network and given access to secure system resources. See Figure 13.19.

Notice that the examples of biometric security listed in Figure 13.19 are rated according to the degree of intrusiveness (how much the technique interrupts a user) and the relative amount of effort required by the user to authenticate. Also, the relative accuracy and cost of each are assessed. As you can see, trade-offs in these four areas exist in every example. Whereas face geometry is judged easy on the user in terms of intrusiveness and effort, its accuracy is not considered as high as that of other methods. Biometrics is still in its infancy, and many new technologies are being developed to improve on accuracy while minimizing user effort.

Computer Failure Controls

"Sorry, our computer systems are down" is a well-known phrase to many end users. A variety of controls can prevent such computer failure or minimize its effects. Computer systems fail for several reasons—power failures, electronic circuitry malfunctions, telecommunications network problems, hidden programming errors, computer viruses, computer operator errors, and electronic vandalism. For example, computers are available with automatic and remote maintenance capabilities. Programs of preventive maintenance of hardware and management of software updates are commonplace. A backup computer system capability can be arranged with *disaster recovery organizations.* Major hardware or software changes are usually carefully scheduled and implemented to avoid problems. Finally, highly trained data center personnel and the use of performance and security management software help keep a company's computer system and networks working properly.

Fault-Tolerant Systems

Many firms also use **fault-tolerant** computer systems that have redundant processors, peripherals, and software that provide a *fail-over* capability to back up components in the event of system failure. This system may provide a *fail-safe* capability so that the computer system continues to operate at the same level even if there is a major hardware or software failure. Many fault-tolerant computer systems, however, offer a *fail-soft* capability so that the computer system can continue to operate at a reduced but acceptable level in the event of a major system failure. Figure 13.20 outlines some of the fault-tolerant capabilities used in many computer systems and networks.

What If the Internet Went Down . . . and Didn't Come Back Up?

Yes. We know we all rely on the Internet. But how much?

Imagine, if you will, a world with no Internet. No e-mail. No e-commerce. And no BlackBerrys. E-mail would be supplanted by snail mail; cell phones by land lines.

Now imagine what the future would look like. Futurists say virtual business services of all sorts, accounting, payroll and even sales would come to a halt, as would many companies.

If the Internet were to cease functioning today, the effect would be similar for many people. Increasingly, we are growing up with ubiquitous communication, information at our fingertips, and shopping at the click of a mouse. Many businesses would also come to a crashing halt. Customer lists consisting solely of e-mail addresses are singularly useless without e-mail, and online brochures and catalogs are simply computer wallpaper without the wherewithal to allow potential customers to browse them. And for software developers and others who rely on customer downloads and online credit card payments, the business world would come to an end until they completely rebuilt their business model.

Yes, the corporate landscape would certainly have a very different look, and a lot of businesses would definitely not be able to adjust. Amazon.com? Forget it. E-Bay—gone. E-Trade—bye-bye. In fact, any online shopping would be toast, unless it was conducted through a proprietary service using its dedicated lines (at considerably higher cost). So would payment systems that depend on Internet connections, payroll services, online banking, and Web-based backup services and customer support.

And a lot of media outlets that have moved most of their operations online would scramble madly to resurrect hard copy and its associated advertising revenues.

And don't even think about the blind panic of last-minute Christmas shopping without all those e-tailers promising next-day delivery!

On the plus side, we'd be forever rid of those infernal "male member enhancement" e-mail messages and the kind offers of millions of dollars from strangers on foreign shores that clutter up our inboxes. "One of the things which would disappear with the Internet would be machine-made fame. Modern mass communications have created centripetal attention structures that bottle celebrity, and celebrities, for sale," says futurist Thornton May. "Our adoration of princesses, movie stars, and basketball players would come to an end. This is not necessarily a bad thing."

Could we really go back to the pre-Internet days over time? "We wouldn't do that. We'd recreate the Internet," says May. He adds, "Would Net2 that would be erected to replace Net1 be better? And how long would it take to get Net2 up?"

And then how long would it take us to catch up with our e-mail?

Source: Adapted from Lynn Greiner, "What If the Internet Went Down . . . and Didn't Come Back Up?" *CIO*, January 15, 2008.

FIGURE 13.20
Methods of fault tolerance in computer-based information systems.

Layer	Threats	Fault-Tolerant Methods
Applications	Environment, hardware, and software faults	Application-specific redundancy and rollback to previous checkpoint
Systems	Outages	System isolation, data security, system integrity
Databases	Data errors	Separation of transactions and safe updates, complete transaction histories, backup files
Networks	Transmission errors	Reliable controllers; safe asynchrony and handshaking; alternative routing; error-detecting and error-correcting codes
Processes	Hardware and software faults	Alternative computations, rollback to checkpoints
Files	Media errors	Replication of critical data on different media and sites; archiving, backup, retrieval
Processors	Hardware faults	Instruction retry; error-correcting codes in memory and processing; replication; multiple processors and memories

Disaster Recovery

Natural and human-made disasters do happen. Hurricanes, earthquakes, fires, floods, criminal and terrorist acts, and human error can all severely damage an organization's computing resources and thus the health of the organization itself. Many companies, especially online e-commerce retailers and wholesalers, airlines, banks, and Internet service providers, for example, are crippled by losing even a few hours of computing power. Many firms could survive only a few days without computing facilities. That's why organizations develop **disaster recovery** procedures and formalize them in a *disaster recovery plan*. It specifies which employees will participate in disaster recovery and what their duties will be; what hardware, software, and facilities will be used; and the priority of applications that will be processed. Arrangements with other companies for use of alternative facilities as a disaster recovery site and off-site storage of an organization's databases are also part of an effective disaster recovery effort.

System Control and Audits

Two final security management requirements that need to be mentioned are the development of information system controls and auditing business systems. Let's take a brief look at these two security measures.

Information System Controls

Information system controls are methods and devices that attempt to ensure the accuracy, validity, and propriety of information system activities. Information system (IS) controls must be developed to ensure proper data entry, processing techniques, storage methods, and information output. Thus, IS controls are designed to monitor and maintain the quality and security of the input, processing, output, and storage activities of any information system. See Figure 13.21.

For example, IS controls are needed to ensure the proper entry of data into a business system and thus avoid the garbage in, garbage out (GIGO) syndrome. Examples include passwords and other security codes, formatted data entry screens, and audible error signals. Computer software can include instructions to identify incorrect, invalid, or improper input data as it enters the computer system. For example, a data entry program can check for invalid codes, data fields, and transactions, and conduct "reasonableness checks" to determine if input data exceed specified limits or are out of sequence.

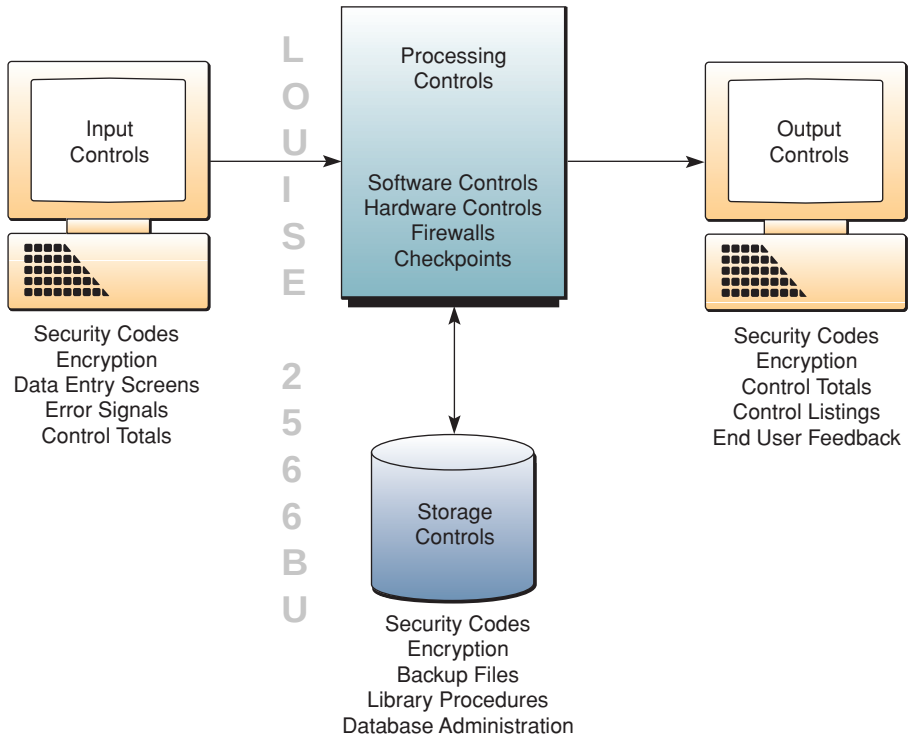


FIGURE 13.21
Examples of information system controls. Note that they are designed to monitor and maintain the quality and security of the input, processing, output, and storage activities of an information system.

FIGURE 13.22
How to protect yourself from cyber-crime and other computer security threats.

Security Management for Internet Users

1. Use antivirus and firewall software and update it often to keep destructive programs off your computer.
2. Don't allow online merchants to store your credit card information for future purchases.
3. Use a hard-to-guess password that contains a mix of numbers and letters, and change it frequently.
4. Use different passwords for different Web sites and applications to keep hackers guessing.
5. Install all operating system patches and upgrades.
6. Use the most up-to-date version of your Web browser, e-mail software, and other programs.
7. Send credit card numbers only to secure sites; look for a padlock or key icons at the bottom of the browser.
8. Use a security program that gives you control over "cookies" that send information back to Web sites.
9. Install firewall software to screen traffic if you use DSL or a cable modem to connect to the Net.
10. Don't open e-mail attachments unless you know the source of the incoming message.

Auditing IT Security

IT security management should be periodically examined, or audited, by a company's internal auditing staff or external auditors from professional accounting firms. Such audits review and evaluate whether proper and adequate security measures and management policies have been developed and implemented. This process typically involves verifying the accuracy and integrity of the software used, as well as the input of data and output produced by business applications. Some firms employ special computer security auditors for this assignment. They may use special test data to check processing accuracy and the control procedures built into the software. The auditors may develop special test programs or use audit software packages.

Another important objective of business system audits is testing the integrity of an application's *audit trail*. An **audit trail** can be defined as the presence of documentation that allows a transaction to be traced through all stages of its information processing. This journey may begin with a transaction's appearance on a source document and end with its transformation into information in a final output document or report. The audit trail of manual information systems is quite visible and easy to trace. However, computer-based information systems have changed the form of the audit trail. Now auditors must know how to search electronically through disk and tape files of past activity to follow the audit trail of today's networked computer systems.

Many times, this *electronic audit trail* takes the form of *control logs* that automatically record all computer network activity on magnetic disk or tape devices. This audit feature can be found on many online transaction processing systems, performance and security monitors, operating systems, and network control programs. Software that records all network activity is also widely used on the Internet, especially the World Wide Web, as well as on corporate intranets and extranets. Such an audit trail helps auditors check for errors or fraud, but also helps IS security specialists trace and evaluate the trail of hacker attacks on computer networks.

Figure 13.22 summarizes 10 security management steps you can take to protect your computer system resources from hacking and other forms of cyber-crime.

Summary

- **Ethical and Societal Dimensions.** The vital role of information technologies and systems in society raises serious ethical and societal issues in terms of their impact on employment, individuality, working conditions, privacy, health, and computer crime, as illustrated in Figure 13.2.

  Employment issues include the loss of jobs—a result of computerization and automation of work—versus

the jobs created to supply and support new information technologies and the business applications they make possible. The impact on working conditions involves the issues of computer monitoring of employees and the quality of the working conditions of the jobs that use information technologies heavily. The effect of IT on individuality addresses the issues of the depersonalization, regimentation, and inflexibility of some computerized business systems.

Employees' heavy use of computer workstations for long periods raises issues about and may cause work-related health disorders. The use of IT to access or collect private information without authorization, as well as for computer profiling, computer matching, computer monitoring, and computer libel and censorship, raises serious privacy issues. Computer crime issues surround activities such as hacking, computer viruses and worms, cyber-theft, unauthorized use at work, software piracy, and piracy of intellectual property.

Managers, business professionals, and IS specialists can help solve the problems of improper use of IT by assuming their ethical responsibilities for the ergonomic design, beneficial use, and enlightened management of information technologies in our society.

- **Ethical Responsibility in Business.** Business and IT activities involve many ethical considerations. Basic principles of technology and business ethics can serve as guidelines for business professionals when dealing with ethical business issues that may arise in the widespread use of information technology in business and society. Examples include theories of corporate social responsibility, which outline the ethical responsibility of management and employees to a company's stockholders, stakeholders, and society, and the four principles of technology ethics summarized in Figure 13.4.
- **Security Management.** One of the most important responsibilities of the management of a company is to ensure the security and quality of its IT-enabled business activities. Security management tools and policies can ensure the accuracy, integrity, and safety of the information systems and resources of a company and thus minimize errors, fraud, and security losses in its business activities. Examples mentioned in the chapter include the use of encryption of confidential business data, firewalls, e-mail monitoring, antivirus software, security codes, backup files, security monitors, biometric security measures, computer failure controls, fault-tolerant systems, disaster recovery measures, information system controls, and security audits of business systems.

Key Terms and Concepts

These are the key terms and concepts of this chapter. The page number of their first explanation is in parentheses.

1. Antivirus software (564)
2. Audit trail (570)
3. Backup files (565)
4. Biometric security (566)
5. Business ethics (528)
6. Computer crime (534)
7. Computer matching (548)
8. Computer monitoring (551)
9. Computer virus (542)
10. Cyber law (550)
11. Disaster recovery (569)
12. Distributed denial of service (DDOS) (561)
13. Encryption (559)
14. Ergonomics (553)
15. Ethical foundations (528)
16. Fault tolerant (567)
17. Firewall (560)
18. Flaming (550)
19. Hacking (535)
20. Information system controls (569)
21. Intellectual property theft (541)
22. Opt-in/Opt-out (546)
23. Passwords (565)
24. Security management (555)
25. Societal solutions (553)
26. Software piracy (540)
27. Spamming (550)
28. Spyware/Adware (544)
29. System security monitor (566)
30. Unauthorized use (538)

Review Quiz

Match one of the key terms and concepts listed previously with one of the brief examples or definitions that follow. Try to find the best fit for the answers that seem to fit more than one term or concept. Defend your choices.

____ 1. Ensuring the accuracy, integrity, and safety of business/IT activities and resources.

____ 2. Control totals, error signals, backup files, and security codes are examples.

____ 3. Software that can control access and use of a computer system.

____ 4. A computer system can continue to operate even after a major system failure if it has this capability.

____ 5. A computer system that serves as a filter for access to and from other networks by a company's networked computers.

____ 6. Laws and regulations focused on issues related to the Internet and other forms of networked communications.

____ 7. The presence of documentation that allows a transaction to be traced through all stages of information processing.

____ 8. Using your voice or fingerprints to identify yourself electronically.

____ 9. A plan to continue IS operations during an emergency.

____ 10. Scrambling data during its transmission.

____ 11. Ethical choices may result from decision-making processes, cultural values, or behavioral stages.

____ 12. Managers must confront numerous ethical questions in their businesses.

____ 13. Sending unsolicited e-mail indiscriminately.

____ 14. Software that can infect a machine and transmit private information back to its owner.

____ 15. Two different perspectives on the use of private information.

____ 16. Using computers to identify individuals that fit a certain profile.

____ 17. Using computers to monitor the activities of workers.

____ 18. Overwhelming a Web site with requests for service from captive computers.

____ 19. Using computers and networks to steal money, services, software, or data.

____ 20. Using company computers to access the Internet during work hours for personal business.

____ 21. Unauthorized copying of software.

____ 22. Unauthorized copying of copyrighted material.

____ 23. Electronic breaking and entering into a computer system.

____ 24. A program that makes copies of itself and destroys data and programs.

____ 25. Finds and eliminates computer viruses.

____ 26. Sending extremely critical, derogatory, and vulgar e-mail messages.

____ 27. Designing computer hardware, software, and workstations that are safe, comfortable, and easy to use.

____ 28. Applications of information technology that have beneficial effects for society at large.

____ 29. Duplicate files of programs or data that are periodically copied and stored elsewhere in case the original is damaged and needs to be restored.

____ 30. A piece of data, known only to an authorized user, that is used to gain access to a system.

Discussion Questions

1. What can be done to improve the security of business uses of the Internet? Give several examples of security measures and technologies you would use.
2. What potential security problems do you see in the increasing use of intranets and extranets in business? What might be done to solve such problems? Give several examples.
3. Refer to the real-world example about copying CDs and music downloading in the chapter. Is copying music CDs an ethical practice? How about Internet music downloading? Explain.
4. What are your major concerns about computer crime and privacy on the Internet? What can you do about it? Explain.
5. What is disaster recovery? How could it be implemented at your school or work?
6. Refer to the Real World Case on IT and ethics in the chapter. Most or all companies have an ethics and compliance program of some sort, but not all of them "live" by it. What does it take for a company to take this next step? What is the role of IT in that scenario?
7. Is there an ethical crisis in business today? What role does information technology play in unethical business practices?
8. What are several business decisions that you will have to make as a manager that have both ethical and IT dimensions? Give examples to illustrate your answer.
9. Refer to the Real World Case on endpoint security in the chapter. How do companies strike a balance between providing users with access to the information they need in the form that is most useful to them, while at the same time enforcing adequate security? What issues should organizations consider when making this decision?
10. What would be examples of one positive and one negative effect of the use of information technologies in each of the ethical and societal dimensions illustrated in Figure 13.2? Explain several of your choices.

Analysis Exercises

1. Problems with Passwords

Authentication

Network and application managers need to know who is accessing their systems to determine appropriate access levels. Typically, they require that users create secret passwords. A secret password, known only to the user, allows an administrator to feel confident that a user is who the user says he or she is. Systems administrators even have the authority to determine the characteristics of passwords. For example, they may set a minimum length and require that a password include numbers, symbols, or mixed letter case. They may also require that a user change his or her password every few weeks or months. These approaches have numerous problems:

- Users often forget complicated or frequently changing passwords, resulting in frequent calls to a help desk. The help-desk employee then faces the burden of identifying the employee by some other means and resetting the password. This process takes time and is subject to social engineering.
- Users may write down their passwords. However, this leaves passwords subject to discovery and theft.
- Users often pick the same password for many different accounts, which means that someone who discovers one of these passwords then has the "keys" to all the accounts.
- Users may pick an easy-to-remember password, which is easy to anticipate and therefore easy to guess. Password-cracking programs cycle through entire dictionaries of English language words and common word/number combinations such as "smart1" or "2smart4U."
- Users may give away their passwords over the phone (social engineering) or via e-mail (phishing, a type of social engineering) to individuals representing themselves as a system administrator. Perhaps you have already received e-mails purportedly from a financial institution claiming identity or account difficulties and asking you to "reconfirm" your account information on their authentic-looking Web site.

As you can see, using passwords to identify a person is fraught with problems. Here are some alternatives to explore. Look up each authentication approach listed below on the Internet, describe the method in your own words (be sure to cite your sources), and briefly list the advantages and disadvantages.

a. Biometrics (biological measuring)
b. Smart cards
c. Biochips

LUTTRELL, SONYA LOUISE 256668U

2. Your Internet Job Rights

Three Ethical Scenarios

Whether you're an employer or an employee, you should know what your rights are when it comes to Internet use in the workplace. Mark Grossman, a Florida attorney who specializes in computer and Internet law, gives answers to some basic questions.

- **Scenario 1:** Nobody told you that your Internet use in the office was being monitored. Now you've been warned you'll be fired if you use the Internet for recreational surfing again. What are your rights?
  Bottom line: When you're using your office computer, you essentially have no rights. You'd have a tough time convincing a court that the boss invaded your privacy by monitoring your use of the company PC on company time. You should probably be grateful you got a warning.
- **Scenario 2:** Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?
  Bottom line: Although the law isn't fully developed in this area, courts are taking a straightforward approach: If it's a company computer, the company can control the way it's used. You don't need an Internet usage policy to prevent inappropriate use of your company computers. To protect yourself in the future, distribute an Internet policy to your employees as soon as possible.
- **Scenario 3:** Employee John Doe downloads adult material to his PC at work, and employee Jane Smith sees it. Smith then proceeds to sue the company for sexual harassment. As the employer, are you liable?
  Bottom line: Whether it comes from the Internet or from a magazine, adult material has no place in the office. So Smith could certainly sue the company for allowing a sexually hostile environment. The best defense is for the company to have an Internet usage policy that prohibits visits to adult sites. Of course, you have to follow through. If someone is looking at adult material in the office, you must at least send the offending employee a written reprimand. If the company lacks a strict Internet policy, though, Smith could prevail in court.

a. Do you agree with the advice of attorney Mark Grossman in each of the scenarios? Why or why not?
b. What would your advice be? Explain your positions.
c. Identify any ethical principles you may be using to explain your position in each of the scenarios.

3. Exploiting Security Weaknesses

Social Engineering

An employee who needs permission to access an electronic workspace, database, or other information

systems resource typically fills in a request form and obtains approval from the responsible manager. The manager then routes the request to one of the system's administrators.

Highly trusted and well-trained systems administrators spend a significant amount of time doing nothing more technical than adding or removing names from access control lists. In large organizations, it's not unusual for systems administrators to have never met any of the people involved in a specific request. The administrators may not even work in the same office.

Hackers have learned to take advantage of this approach to access authorization. They begin by probing an organization. The hacker doesn't expect to compromise the system during this initial probe. He or she just starts by making a few phone calls to learn who is responsible for granting access and how to apply. A little more probing helps the hacker learn who's who within the organization's structure. Some organizations even post this information online in the form of employee directories. With this information in hand, the hacker knows whom to talk to, what to ask for, and what names to use to sound convincing. The hacker is now ready to try to impersonate an employee and trick a systems administrator into revealing a password and unwittingly granting unauthorized access.

Organizations determine who needs access to which applications. They also need a system through which they can authenticate the identity of an individual making a request. Finally, they need to manage this process both effectively and inexpensively.

a. Describe the business problems that this exercise presents.
b. Suggest several ways to reduce an organization's exposure to social engineering.
c. Prepare an orientation memo to new hires in your IT department describing "social engineering." Suggest several ways employees can avoid being tricked by hackers.

4. Privacy Statements

The Spyware Problem

Web surfers may feel anonymous as they use the Internet, but that feeling isn't always justified. IP addresses, cookies, site log-in procedures, and credit card purchases all help track how often users visit a site and what pages they view. Some companies go further.

Some free screensaver software and peer-to-peer file sharing come with "spyware" embedded within their applications. Once loaded, these applications run in the background. What they actually track depends on the specific software. To stay on the "right side" of U.S. law, these companies outline their software's functions in general terms and include this information in the small print within their end-user licensing agreement (EULA) and/or privacy policy. In fact, these agreements may even include a stipulation that users not disable any part of their software as a condition for free use.

Because most users don't read these policies, they have no idea what privacy rights they may have given up. They indeed get their free file-sharing program or screen saver, but they may be getting a lot more. Some spyware programs even remain on hard drives and stay active after users have uninstalled their "free" software.

a. Use a search engine to search for "spyware," "spyware removal," "adware," or other related terms. Prepare a one-page summary of your results. Include URLs for online sources.
b. Select three of your favorite Web sites and print out their privacy policies. What do they share in common? How do they differ?
c. Write your own Web site privacy policy, striking a balance between customer and business needs.

REAL WORLD CASE 3

Ethics, Moral Dilemmas, and Tough Decisions: The Many Challenges of Working in IT

What Bryan found on an executive's computer six years ago still weighs heavily on his mind. He's particularly troubled that the man he discovered using a company PC to view pornography of Asian women and of children was subsequently promoted and moved to China to run a manufacturing plant. "To this day, I regret not taking that stuff to the FBI." It happened when Bryan, who asked that his last name not be published, was IT director at the U.S. division of a $500 million multinational corporation based in Germany.

The company's Internet usage policy, which Bryan helped develop with input from senior management, prohibited the use of company computers to access pornographic or adult-content Web sites. One of Bryan's duties was to use products from SurfControl PLC to monitor employee Web surfing and to report any violations to management.

Bryan knew that the executive, who was a level above him in another department, was popular within both the U.S. division and the German parent. Yet when the tools turned up dozens of pornographic Web sites visited by the executive's computer, Bryan followed the policy.

"That's what it's there for. I wasn't going to get into trouble for following the policy," he reasoned.

Bryan's case is a good example of the ethical dilemmas that IT workers may encounter on the job. IT employees have privileged access to digital information, both personal and professional, throughout the company, and they have the technical prowess to manipulate that information. That gives them both the power and responsibility to monitor and report employees who break company rules. IT professionals may also uncover evidence that a coworker is, say, embezzling funds, or they could be tempted to peek at private salary information or personal e-mails. There's little guidance, however, on what to do in these uncomfortable situations.

In the case of the porn-viewing executive, Bryan didn't get into trouble, but neither did the executive, who came up with "a pretty outlandish explanation" that the company accepted, Bryan says. He considered going to the FBI, but the Internet bubble had just burst and jobs were hard to come by. "It was a tough choice," Bryan says. "But I had a family to feed."

Perhaps it would ease Bryan's conscience to know that he did just what labor attorney Linn Hynds, a senior partner at Honigman Miller Schwartz and Cohn LLP, would have advised in his case. "Let the company handle it," she says. "Make sure you report violations to the right person in your company, and show them the evidence. After that, leave it to the people who are supposed to be making that decision." Ideally, corporate policy takes over where the law stops, governing workplace ethics to clear up gray areas and remove personal judgment from the equation as much as possible.

"If you don't set out your policy and your guidelines, if you don't make sure that people know what they are and understand them, you're in no position to hold workers accountable," says John Reece, a former chief information officer at the Internal Revenue Service and Time Warner Inc.

Having clear ethical guidelines also lets employees off the hook emotionally if the person they discover breaking the policy is a friend, someone who reports to them directly, or a supervisor, says Reece, who is now head of consultancy at John C. Reece and Associates LLC. Organizations that have policies in place often focus on areas where they had trouble in the past or emphasize whatever they are most worried about. When Reece was at the IRS, for example, the biggest emphasis was on protecting the confidentiality of taxpayer information.

At the U.S. Department of Defense, policies usually emphasize procurement rules, notes Stephen Northcutt, president of the SANS Technology Institute and author of *IT Ethics Handbook: Right and Wrong for IT Professionals*. Adding to the complexity, an organization that depends on highly skilled workers might be more lenient. When Northcutt worked in IT security at the Naval Surface Warfare Center in Virginia, it was a rarefied atmosphere of highly sought-after PhDs. "I was told pretty clearly that if I made a whole lot of PhDs very unhappy so that they left, the organization wouldn't need me anymore," says Northcutt.

Of course, that wasn't written in any policy manual, so Northcutt had to read between the lines. "The way I interpreted it was: Child pornography, turn that in," he says. "But if the leading mathematician wants to download some pictures of naked girls, they didn't want to hear from me."

Northcutt says that he did find child porn on two occasions and that both events led to prosecution. As for other offensive photos that he encountered, Northcutt pointed out to his superiors that there might be a legal liability, citing a Supreme Court decision that found that similar pictures at a military installation indicated a pervasive atmosphere of sexual harassment. That did the trick. "Once they saw that law was involved, they were more willing to change culture and policy," Northcutt says.

When policies aren't clear, ethical decisions are left to the judgment of IT employees, which varies by person and the particular circumstances. For example, Gary, a director of technology at a nonprofit organization in the Midwest, flat-out refused when the assistant chief executive officer wanted to use a mailing list that a new employee had stolen from her former employer. Yet Gary, who asked that his last name not be used, didn't stop his boss from installing unlicensed software on PCs for a short time, although he refused to do it himself. "The question is, how much was it really going to hurt anybody? We were still going to have 99.5 percent compliant software. I was OK with that."

He says he uninstalled it, with his boss's approval, as soon as he could, which was about a week later.

Northcutt argues that the IT profession should have two things that professions such as law or accounting have had for years: a code of ethics and standards of practice. That way, when company policy is nonexistent or unclear, IT professionals still have standards to follow.

That might be useful for Tim, a systems administrator who works at a Fortune 500 agricultural business. When Tim, who asked that his last name not be published, happened across an unencrypted spreadsheet of salary information on a manager's PC, he copied it. He didn't share the information with anyone or use it to his advantage. It was an impulsive act, he admits, that stemmed from frustration with his employer. "I didn't take it for nefarious reasons; I just took it to prove that I could," he says.

Tim's actions point to a disturbing trend: IT workers are justifying their ethically questionable behavior. That path can end in criminal activity, says fraud investigator Chuck Martell. "We started seeing a few cases about seven or eight years ago," says Martell, managing director of investigative services at Veritas Global LLC, a security firm in Southfield, Michigan. "Now we're investigating a tremendous amount of them."

Whole Foods Market Chairman and CEO John Mackey spent years earning a positive reputation as a corporate leader who was not afraid to take a stand on ethics issues. Before other companies figured out that it pays to be environmentally friendly, Whole Foods led by setting standards for humane animal treatment. In 2006, Mackey took the bold step of reducing his own annual salary to one dollar, pledging money instead for an emergency fund for his staff. Not shy about expressing his views, Mackey challenged leading thinkers, like Nobel Prize–winner Milton Friedman, on business ethics issues. Like many leaders, Mackey seemed to relish the public spotlight.

On July 20, 2007, however, Mackey got more than he bargained for in terms of publicity. *The Wall Street Journal* reported that Mackey had long used the pseudonym "Rahodeb" to make postings in Yahoo Finance forums that flattered his own company and leveled criticisms against the competition. Serious financial and possibly legal repercussions continue to unfold from this incident, and the final consequences may not be known for some time.

Amid the furor that followed this disclosure of Mackey's secret online alias, it is vital that we not lose sight of the critical issues it raises about ethics and leadership in a rapidly evolving business world. There is no question that the current climate has prompted many more companies to tackle ethics issues.

By now, "business ethics" is an established part of doing business, not just in the United States, but also increasingly around the world. People no longer joke that "business ethics is an oxymoron," as society has come not merely to expect, but to demand, that business conduct itself according to basic rules of ethics and integrity. Business will always need to pay attention to ethics and leadership, but these lessons are continually challenged by new developments, including technological advances that promote new kinds of communication online. Business leaders cannot afford to overlook these challenges, as even a single misstep can be enough to undo a reputation for ethical leadership.

Source: Adapted from Tam Harbert, "Ethics in IT: Dark Secrets, Ugly Truths—and Little Guidance," *Computerworld*, October 29, 2007; and David Schmidt, "What Is the Moral Responsibility of a Business Leader?" *CIO Magazine*, September 12, 2007.

CASE STUDY QUESTIONS

1. Companies are developing ethical policies and guidelines for legal reasons, but also to clarify what is acceptable and what is not. Do you think any of the issues raised in the case required clarification? Would you take exception to any of them being classified as inappropriate behavior? Why do you think these things happen anyway?
2. In the first example (Bryan's), it is apparent that he did not believe justice had been ultimately served by the decision his company made. Should he have taken the issue to the authorities? Or was it enough that he reported the problem through the proper channels and let the organization handle it, as was the recommendation of Linn Hynds? Provide a rationale for the position you are willing to take on this matter.
3. In the case, Gary chose not to stop his boss from installing unlicensed software, although he refused to do it himself. If installing unlicensed software is wrong, is there any difference between refusing to do it versus not stopping somebody else? Do you buy his argument that it was not really going to hurt anybody? Why or why not?

REAL WORLD ACTIVITIES

1. Go online to follow up on John Mackey's story and search for other instances of debatable behavior where IT has been an important factor. Are the ones featured in the case exceptions, or are these occurrences becoming more and more common? How do organizations seem to be coping with these issues? What type of responses did you find? Prepare a report to summarize your findings.
2. The case features many examples of what is arguably unethical behavior, including child pornography, accessing adult content on company-owned equipment, installing unlicensed software, and so on. Are some of these practices "more wrong" than others? Is there any one that you would not consider problematic? Break into small groups to discuss these questions, and make a list of other ethical problems involving IT that were not mentioned in the case.

REAL WORLD CASE 4

Raymond James Financial, BCD Travel, Houston Texans, and Others: Worrying about What Goes Out, Not What Comes In

LUTTRELL, SONYA LOUISE 256668U

It's not what's coming into the corporate network that concerns Gene Fredriksen; it's what's going out. For the chief security officer at securities brokerage Raymond James Financial Inc. in St. Petersburg, Florida, leakage of sensitive customer data or proprietary information is the new priority. The problem isn't just content within e-mail messages, but the explosion of alternative communication mechanisms that employees are using, including instant messaging, blogs, FTP transfers, Web mail, and message boards. It's not enough to just monitor e-mail, Fredriksen says. "We have to evolve and change at the same pace as the business," he explains. "Things are coming much faster."

So Fredriksen is rolling out a network-based outbound content monitoring and control system. The software, from San Francisco–based Vontu Inc., sits on the network and monitors traffic in much the same way that a network-based intrusion-detection system would. Rather than focusing on inbound traffic, however, Vontu monitors the network activity that originates from Raymond James's 16,000 users. It examines the contents of each network packet in real time and issues alerts when policy violations are found.

Network-based systems do more than just rule-based scanning for Social Security numbers and other easily identifiable content. They typically analyze sensitive documents and content types and generate a unique fingerprint for each. Administrators then establish policies that relate to that content, and the system uses linguistic analysis to identify sensitive data and enforce those policies as information moves across the corporate LAN. The systems can detect both complete documents and "derivative documents," such as an IM exchange in which a user has pasted a document fragment.

When BCD Travel began to investigate what it would take to get Payment Card Industry (PCI) certification for handling customer credit card data, Brian Flynn, senior vice president of technology, realized that he didn't really know how his employees were handling such information. Not only could PCI certification be denied, but the travel agency's reputation and business could also be harmed. At the National Football League's Houston Texans, IT Director Nick Ignatiev came to the same realization as he investigated PCI certification.

In both cases, vendors they'd been working with suggested a new technology: outbound content management tools that look for proprietary information that might be leaving the company via e-mail, instant messaging, or other avenues. Flynn started to use Reconnex's iGuard network appliance, with vivid results. "It was a shock to see what was going out, and that gave us the insight to take action," he says. After Ignatiev examined his message flow using Palisade Systems's PacketSure appliance, he too realized that his employees needed to do a better job protecting critical data, including customer credit cards, scouting reports, and team rosters.

How does the technology work? Basically, the tools filter outgoing communication across a variety of channels, such as e-mail and IM, to identify sensitive information. They're based on some of the same technologies—like pattern matching and contextual text search—that help antivirus and antispam tools block incoming threats.

Tools typically come with basic patterns already defined for personally identifiable information, such as Social Security and credit card numbers, as well as templates for commonly private information, such as legal filings, personnel data, and product testing results.

Companies typically look for three types of information using these tools, notes Paul Kocher, president of the Cryptography Research consultancy. The first, and easiest, type is personally identifiable information, such as Social Security numbers and credit card information. The second type is confidential company information, such as product specifications, payroll information, legal files, or supplier contracts. Although this information is harder to identify, most tools can uncover patterns of language and presentation when given enough samples, Kocher notes. The third category is inappropriate use of company resources, such as potentially offensive communications involving race.

The traditional security methods may restrict sensitive data to legitimate users, but Flynn and Ignatiev found that even legitimate users were putting the data, and their companies, at risk. At BCD Travel, a corporate travel service, nearly 80 percent of its 10,000 employees work in call centers and thus have legitimate access to sensitive customer information. BCD and the Texans did not find malicious activity; instead, they found people who were unaware of security risks, such as sending a customer's credit card number by e-mail to book a flight or room from a vendor that didn't have an online reservations system.

Fidelity Bancshares Inc. in West Palm Beach, Florida, is using the message-blocking feature in PortAuthority from PortAuthority Technologies Inc. in Palo Alto, California. Outbound e-mail messages that contain Social Security numbers, account numbers, loan numbers, or other personal financial data are intercepted and returned to the user, along with instructions on how to send the e-mail securely.

Joe Cormier, vice president of network services, says he also uses PortAuthority to catch careless replies. Customers often send in questions and include their account information. "The customer service rep would reply back without modifying the e-mail," he says.

"The challenge with any system like this is they're only as valuable as the mitigation procedures you have on the back end," notes Fredriksen. Another key to success is educating users about monitoring to avoid "Big Brother" implications. "We are making sure that the users understand why we implement systems like this and what they're being used for, he says.

Mark Rizzo, vice president of operations and platform engineering at Perpetual Entertainment Inc. in San Francisco, learned in a previous job the consequences of not protecting intellectual property. "I have been on the side of things disappearing and showing up at competitors," he says. The start-up online game developer deployed Tablus's Content Alarm to remedy the problem. Rizzo uses it to look for suspicious activity, such as large files that are moving outside the corporate LAN. Now that the basic policies and rules have been set, the system doesn't require much ongoing maintenance, he says. Still, Rizzo doesn't use blocking because he would need to spend significant amounts of time to create more policies in order to avoid false positives.

Although companies in highly regulated industries can justify investing in outbound content monitoring and blocking tools, other organizations may have to sharpen their pencils to justify the cost. These are very expensive solutions to deploy. Fredriksen, who built a system to support 16,000 users, says that for a setup with about 20,000 users, "you're in the $200,000 range, easily."

With outbound content management tools, "you can build very sophisticated concept filters," says Cliff Shnier, vice president for the financial advisory and litigation practice at Aon Consulting. Typically, the tools come with templates for types of data that most enterprises want to filter, and they can analyze contents of servers and databases to derive filters for company-specific information, he says. (Consulting firms can improve these filters using linguists and subject matter experts.)

As any user of an antispam tool knows, no filter is perfect. "A big mistake is to have too much faith in the tools. They can't replace trust and education," says consultant Kocher. They also won't stop a determined thief, he says.

Even when appropriately deployed, these tools don't create an ironclad perimeter around the enterprise. For example, they can't detect information that flows through Skype voice over IP (VoIP) service or SSL (Secure Sockets Layer) connections, Kocher notes. They can also flood logs with false positives, which makes it hard for IT security staff to identify real problems.

That's why chief information officers should look at outbound content management as a supplemental tool to limit accidental or unknowing communication of sensitive data, not as the primary defense. Fredriksen says that although Vontu is important, it's still just one piece of a larger strategy that includes an overlapping set of controls that Raymond James uses to combat insider threats. "This augments the intrusion–detection and firewall systems we have that control and block specific ports," he says. "It's just a piece. It's not the Holy Grail."

Source: Adapted from Galen Gruman, "Boost Security with Outbound Content Management," *CIO Magazine*, April 9, 2007; and Robert Mitchell, "Border Patrol: Content Monitoring Systems Inspect Outbound Communications," *Computerworld*, March 6, 2006.

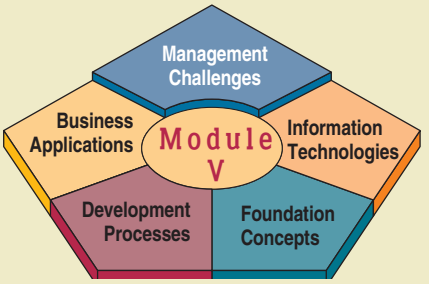
CASE STUDY QUESTIONS

1. Barring illegal activities, why do you think that employees in the organizations featured in the case do not realize themselves the dangers of loosely managing proprietary and sensitive information? Would you have thought of these issues?
2. How should organizations strike the right balance between monitoring and invading their employees' privacy, even if it would be legal for them to do so? Why is it important that companies achieve this balance? What would be the consequences of being too biased to one side?
3. The IT executives in the case all note that outbound monitoring and management technologies are only part of an overall strategy, and not their primary defense. What should be the other components of this strategy? How much weight would you give to human and technological factors? Why?

REAL WORLD ACTIVITIES

1. Technologies such as VoIP used by Skype and similar products make it more difficult to monitor outgoing information. Search the Internet to help you understand these technologies and why these problems arise. Other than banning them, what alternatives would you suggest to companies facing this problem? Prepare a presentation to deliver your recommendations.
2. As a customer of many of the companies noted in the case, or others in the same industries, what is your expectation about the measures and safeguards that these organizations have implemented to protect inappropriate leaking of your personal information? After reading the case, has your expectation changed? Break into small groups with your classmates to discuss these issues.

CHAPTER 14



ENTERPRISE AND GLOBAL MANAGEMENT OF INFORMATION TECHNOLOGY

Chapter Highlights

Section I
Managing Information Technology

Business and IT
Managing Information Technology
Real World Case: Reinventing IT at BP
Business/IT Planning
Managing the IT Function
Organizing IT
Outsourcing and Offshoring IT and IS
Failures in IT Management

Section II
Managing Global IT

The International Dimension
Global IT Management
Real World Case: Cadbury, Forrester Research, A.T. Kearney, and Others: IT Leaders Face New Challenges in a Globalized World
Cultural, Political, and Geoeconomic Challenges
Global Business/IT Strategies
Global Business/IT Applications
Global IT Platforms
Global Data Access Issues
Global Systems Development
Real World Case: Toyota, Procter & Gamble, Hess Corporation, and Others: Retiring CIOs and the Need for Succession Planning
Real World Case: Reinsurance Group of America and Fonterra: Going for Unified Global Operations

Learning Objectives

1. Identify each of the three components of IT management and use examples to illustrate how they might be implemented in a business.
2. Explain how failures in IT management can be reduced by the involvement of business managers in IT planning and management.
3. Identify several cultural, political, and geoeconomic challenges that confront managers in the management of global information technologies.
4. Explain the effect on global business/IT strategy of the trend toward a transnational business strategy by international business organizations.
5. Identify several considerations that affect the choice of IT applications, IT platforms, data access policies, and systems development methods by a global business enterprise.
6. Understand the fundamental concepts of outsourcing and offshoring, as well as the primary reasons for selecting such an approach to IS/IT management.

SECTION I Managing Information Technology

Business and IT

The strategic and operational importance of information technology in business is no longer questioned. As the 21st century unfolds, many companies throughout the world are intent on transforming themselves into global business powerhouses through major investments in global e-business, e-commerce, and other IT initiatives. Thus, there is a real need for business managers and professionals to understand how to manage this vital organizational function. In this section, we explore how the IS function can be organized and managed, and we emphasize the importance of a customer and business value focus for the management of information technologies. Whether you plan to be an entrepreneur and run your own business, a manager in a corporation, or a business professional, managing information systems and technologies will be one of your major responsibilities. See Figure 14.1.

Read the Real World Case on the next page. We can learn a lot from this case about the many challenges faced by a major multinational corporation as it sought to reinvent its IT organization worldwide.

Managing Information Technology

As we have seen throughout this text, information technology is an essential component of business success for companies today; however, information technology is also a vital business resource that must be properly managed. Thus, we have also seen many real-world examples in which the management of information technologies plays a pivotal role in ensuring the success or contributing to the failure of a company's strategic business initiatives. Therefore, managing the information systems and technologies that support the modern business processes of companies today is a major challenge for both business and IT managers and professionals.

How should information technology be managed? Figure 14.2 illustrates one popular approach to **managing information technology** in a large company. This managerial approach has three major components:

- **Managing the Joint Development and Implementation of Business/IT Strategies.** Led by the CEO (chief executive officer) and CIO (chief information officer), proposals are developed by business and IT managers and professionals regarding the use of IT to support the strategic business priorities of the company. This business/IT planning process *aligns* IT with strategic business goals. The process also includes evaluating the business case for investing in the development and implementation of each proposed business/IT project.
- **Managing the Development and Implementation of New Business/IT Applications and Technologies.** This step is the primary responsibility of the CIO and CTO (chief technology officer). This area of IT management involves managing the processes for information systems development and implementation we discussed in Chapter 12, as well as the responsibility for research into the strategic business uses of new information technologies.
- **Managing the IT Organization and the IT Infrastructure.** The CIO and IT managers share responsibility for managing the work of IT professionals who are typically organized into a variety of project teams and other organizational subunits. In addition, they are responsible for managing the IT infrastructure of hardware, software, databases, telecommunications networks, and other IT resources, which must be acquired, operated, monitored, and maintained.

Let's look at a real-world example.

REAL WORLD CASE 1

Reinventing IT at BP

A few years ago, the CEO of one of the world's largest corporations laid some very tough love on his 500 top managers. Despite having annual revenue of about $300 billion, BP had become, said CEO Tony Hayward, "a serial underperformer" that had "promised a lot but not delivered very much."

At that March 2008 meeting, those same 500 top BP managers also heard a Morgan Stanley oil and gas analyst tell them that while the rest of the energy industry was undertaking rapid change, BP was building a legacy of consistent failure both in finding and extracting new energy, and in refining and marketing finished products. And unless BP transformed its entire global business dramatically and rapidly, the analyst predicted, "BP will not exist in four to five years' time in its current form."

One of the people in that meeting was Dana Deasy, BP's chief information officer and group vice president, who'd joined the company four months earlier as its first global CIO.

As Deasy listened to the sobering comments from his CEO and from a highly influential analyst, he thought about the transformation he had already launched within IT, an organization he thought had become—like the company overall—bloated, passive, unfocused, and unconcerned with performance and accountability.

Deasy wanted to strip out $800 million in expenses from BP's overall IT budget of $3 billion; cut in half the more than 2,000 IT vendors it had; overhaul BP's ranks of 4,200 IT employees; rationalize and reduce the 8,500 applications in use at BP worldwide; and turn IT from a tactical services unit into a business-driven and intimately embedded strategic weapon.

No stranger to challenging CIO roles, Deasy took his post with full knowledge of the tumultuous times ahead. "We were several billion dollars behind our competitors in oil and gas, and there was a real and very pressing concern in the company due to that," Deasy says. Another part of the gap that Tony wanted to see closed was around organizational simplification: fewer layers of management, smaller corporate staffs, and deeper talent across key functions.

Although noting that BP at the time had some great people in IT and some cutting-edge systems for exploration, Deasy also understood that he was going to have to drive enormous change in personnel, processes, and objectives across the entire IT organization in order to support and enhance the larger overhaul taking place across all of BP.

He saw a fundamental problem with the 4,200 IT employees BP had. "What was most startling to me about that number, only 55 percent of those IT professionals were actually BP-badged. The rest were contractors, he says. "So I was really struck by the very deep dependency we had on outside contractors."

Then there was the complexity that lay behind that $3 billion IT budget: "That encompassed everything, from the back office to the coalface," says Deasy, including everything from PCs and networks to the IT that supports refineries.

And so in the face of that sprawl in people, budget, priorities, requirements, business objectives, suppliers, and priorities, and inspired by Hayward's stark assessment of BP managers promising more than they delivered, Deasy committed in late 2007 to a three-year overhaul of every facet of BP's IT operations—an overhaul he and his team ultimately completed in two years.

Now, you might say, "Well, what's the big deal? Anybody starting with a $3 billion budget and a lackluster organization could come in and do a few things and look like a genius." That's naive at best and foolish at worst.

"I viewed this as one of the top 5 CIO jobs in the world, and I fully understood it was a truly daunting challenge. But that's one of the reasons it appealed to me," Deasy says. "Could we make this work?"

"The team will say to this day that it's hard to imagine if we went back two years and looked at what lay before us that this is where we'd be today. And so we chuckle about that and say that if we knew then what we know now about what we'd have to do, we would've said, 'No, that is just not possible.'" The ability to dig into those kinds of massive challenges, knowing there's no "magic answer," is a big part of the IT culture Deasy sees: "So when we got the first $400 million in costs out, our people started to have a completely different strut around themselves and a new confidence, so that when we said, 'Hey, do you think we can find another $400 million?' they grimaced, but they also said, 'Yeah, we can do this. Bring it on.'"

FIGURE 14.1

BP has undertaken a major and wide-ranging transformation of its IT organization.

Source: © Doug Menuez/Getty Images.

LUTTRELL, SONYA LOUISE 256 6BU

Although he had many urgent challenges, Deasy made BP's talent pool his top priority. "We desperately needed a baseline," he explains. "If we were going to impose the types of staggering changes we needed to meet the objectives CEO Tony Hayward was laying out, then we had to know if we had the wherewithal to do it."

There was major turnover within those positions, and Deasy says the biggest and most significant change involves the capabilities of the new BP IT organization. "In just 11 months from the time I arrived here at BP, we replaced 80 percent of the top IT leadership within the organization, with those being the people reporting to me," Deasy says. "In the next level down, we replaced 25 percent of global management in the first year with new people we went out and selectively targeted and brought into BP. And it was very inspiring to be told that, yes, you can go out and hire the best people in the world to help you make this transformation possible. And that's exactly what we did."

In year one, BP's IT was highly decentralized. "The company didn't know it spent $3 billion in total on IT, or that it had 4,200 people in IT," Deasy says. "So we decided the right approach was to go a little draconian, and I just exerted control over all the people and all the spending." I knew that wasn't the right long-term model or cultural model for the company, but in the short term I wanted to be able to get enough control to be able to move to an 'embedded IT' model, which we have today."

Each business unit CIO now works for the business leader and also reports to Deasy. "Accountability No. 1 for those CIOs is that they're there to help deliver enablement through IT to drive new revenue, and also for helping to ensure they're driving standardized shared services to keep our costs down," Deasy says.

"With suppliers, I knew we had way too many from all of our decentralized legacy, and when we tried to round them up we stopped counting at around 2,200," he says. It wasn't only the sheer number; the 20 largest suppliers accounted for only 30 percent of IT spending, so "we ended up with a huge tail," Deasy says.

So in 2009, BP took 65 percent of its annual global IT spending, about $1.5 billion, and put it up for rebid in one year. It let BP cut 1,200 IT suppliers, and Deasy estimates it will end up saving the company $900 million over the next five years.

Deasy contends that the buyer-seller tension he has created is good for both parties, as long as each side is honest with the other about expectations and objectives. "You've got to be realistic: What's a vendor's job over the next five years? Well, when you strip away all the fancy talk, it's to claw back all that money they gave up in our rebids. So in 2010, how do we ensure that we don't lose the value of the efficiency play we worked so hard to establish? How can we take our five application development and application maintenance vendors and ensure they keep improving their service and delivering more value to us?"

"We just spent two very hard years rebuilding this organization, and one thing you learn in transforming an organization is that it's not a linear process," he says. "No sooner do you have contracts done, and they're effective, and they're delivering value, than you have to start the control process again.

"It is not linear—not at all—and that means that once you get to the enablement phase, you have to resist the temptation that makes you think you can just live there forever. And believe me, that temptation is very strong. But you've got to resist it and go back and once again begin to exert control, because by that time the organization is not the same as the one over which you first exerted control. It's a process that has to repeat itself because, as much as it might appear to be linear, I can assure you that it's not."

Source: Adapted from Bob Evans, "BP's IT Transformation," *InformationWeek*, March 8, 2010.

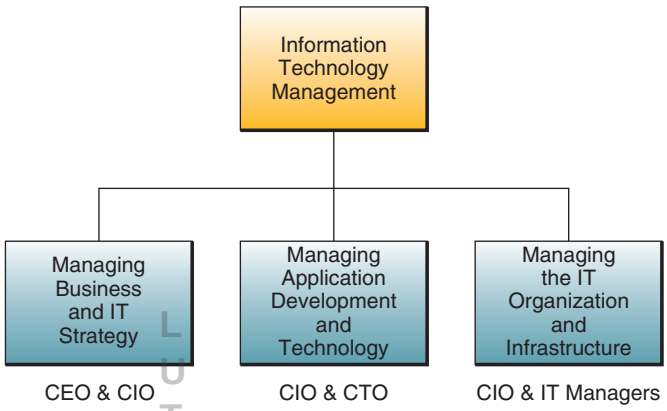
CASE STUDY QUESTIONS

1. The case mentions the dependence of BP's IT organization on external contractors. Why would this be an issue? When is it a good idea for IT departments to hire contractors, and when is it not? Discuss some scenarios.
2. The culture of the IT organization is mentioned as an important issue. How do you think it changed throughout the period covered here? What did it look like when Deasy came on board? What does it look like now?
3. How did BP get to the situation mentioned at the beginning of the transformation process? Does it appear to be the result of a conscious decision? Use examples from the case to illustrate your answer.

REAL WORLD ACTIVITIES

1. Go online and research the performance of BP since the time chronicled in the case. Did the transformation process pay out in the end? What was the role of IT in the outcome, if any? Prepare a report and compare BP's performance with that of their competitors.
2. Go back and reread the last two paragraphs in the case. What do you think Deasy means when he discusses the nonlinear and iterative nature of the process? What does he mean by "temptation"? Break into small groups with your classmates to discuss these questions.

FIGURE 14.2
The major components of information technology management. Note the executives with primary responsibilities in each area.



Avnet Marshall: Managing IT

Figure 14.3 contrasts how Avnet Marshall's information technology management differs from conventional IT management. Notice that it uses the model of IT management illustrated in Figure 14.2. For example, in technology management, Avnet Marshall uses a best-of-breed approach that supports business needs instead of enforcing a standardized and homogeneous choice of hardware, software, database, and networking technologies. In managing its IT organization, Avnet Marshall hires IS professionals who can integrate IT with business. These IS professionals are organized in workgroups around business/IT initiatives that focus on building IT-enabled business services for customers.

Business/IT Planning

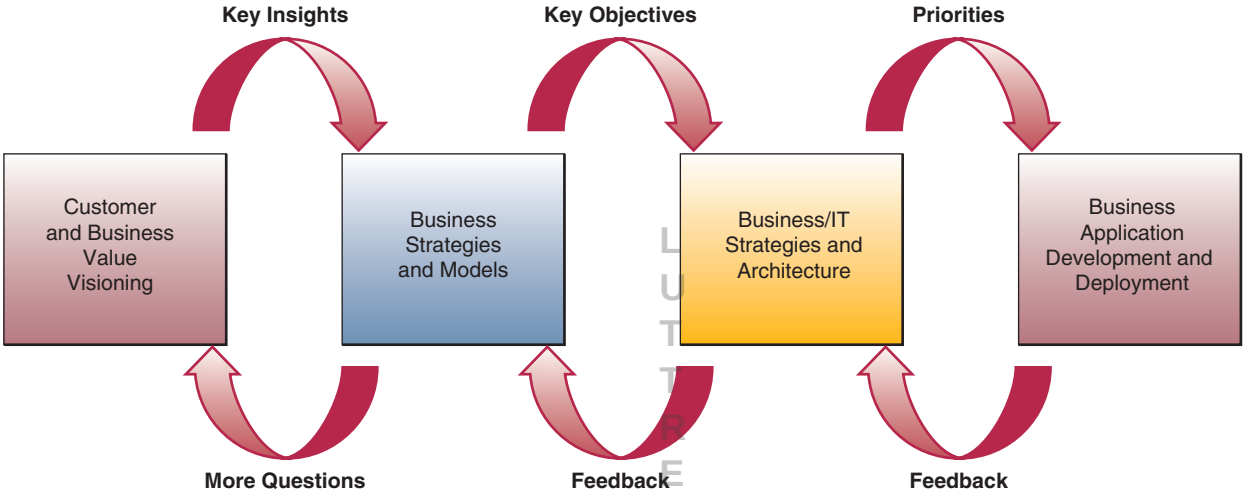
Figure 14.4 illustrates the **business/IT planning process**, which focuses on discovering innovative approaches to satisfying a company's customer value and business value goals. This planning process leads to the development of strategies and business models for new business applications, processes, products, and services. Then a company can

FIGURE 14.3
Comparing conventional and e-business-driven IT management approaches.

IT Management	Conventional Practices	Avnet Marshall's Business/IT Practices
Technology Management	• Approach to IT infrastructure may sacrifice match with business needs for vendor homogeneity and technology platform choices.	• Best-of-breed approach to IT infrastructure in which effective match with business needs takes precedence over commitment to technology platform choices and vendor homogeneity.
Managing the IT Organization	• Hire "best by position" who can bring specific IT expertise. • Departments organized around IT expertise with business liaisons and explicit delegation of tasks. • IT projects have separable cost/value considerations. Funding typically allocated within constraints of yearly budget for IT function.	• Hire "best athletes" IS professionals who can flexibly integrate new IT and business competencies. • Evolving workgroups organized around emerging IT-intensive business initiatives with little explicit delegation of tasks. • IT funding typically based on value proposition around business opportunity related to building services for customers. IT project inseparable part of business initiative.

Source: Adapted from Omar El Sawy, Arvind Malhotra, Sanjay Gosain, and Kerry Young, "IT-Intensive Value Innovation in the Electronic Economy: Insights from Marshall Industries," *MIS Quarterly*, September 1999.

FIGURE 14.4 The business/IT planning process emphasizes a customer and business value focus for developing business strategies and models and an IT architecture for business applications.



develop IT strategies and an IT architecture that supports building and implementing its newly planned business applications.

Both the CEO and the CIO of a company must manage the development of complementary business and IT strategies to meet its customer value and business value vision. This *coadaptation* process is necessary because, as we have seen so often in this text, information technologies are a fast-changing but vital component in many strategic business initiatives. The business/IT planning process has three major components:

- **Strategy Development.** Developing business strategies that support a company's business vision. For example, using information technology to create innovative e-business systems that focus on customer and business value. We will discuss this process in more detail shortly.
- **Resource Management.** Developing strategic plans for managing or outsourcing a company's IT resources, including IS personnel, hardware, software, data, and network resources.
- **Technology Architecture.** Making strategic IT choices that reflect an information technology architecture designed to support a company's business/IT initiatives.

Information Technology Architecture

The **IT architecture** created by the strategic business/IT planning process is a conceptual design, or blueprint, that includes the following major components:

- **Technology Platform.** The Internet, intranets, extranets, and other networks, computer systems, system software, and integrated enterprise application software provide a computing and communications infrastructure, or platform, that supports the strategic use of information technology for e-business, e-commerce, and other business/IT applications.
- **Data Resources.** Many types of operational and specialized databases, including data warehouses and Internet/intranet databases (as reviewed in Chapter 5), store and provide data and information for business processes and decision support.
- **Applications Architecture.** Business applications of information technology are designed as an integrated architecture *or portfolio* of enterprise systems that support strategic business initiatives, as well as cross-functional business processes. For example, an applications architecture should include support for developing and maintaining the interenterprise supply chain applications and integrated

FIGURE 14.5
Comparing business/IT strategic and application planning approaches.

Conventional IT Planning	Avnet Marshall's Business/IT Planning
• Strategic alignment: IT strategy tracks specified enterprise strategy. • CEO endorses IT vision shaped through CIO. • IT application development projects functionally organized as technological solutions to business issues. • Phased application development based on learning from pilot projects.	• Strategic improvisation: IT strategy and enterprise business strategy coadaptively unfold based on the clear guidance of a focus on customer value. • CEO proactively shapes IT vision jointly with CIO as part of e-business strategy. • IT application development projects co-located with e-business initiatives to form centers of IT-intensive business expertise. • Perpetual application development based on continuous learning from rapid deployment and prototyping with end-user involvement.

enterprise resource planning and customer relationship management applications discussed in Chapters 7 and 9.

- **IT Organization.** The organizational structure of the IS function within a company and the distribution of IS specialists are designed to meet the changing strategies of a business. The form of the IT organization depends on the managerial philosophy and business/IT strategies formulated during the strategic planning process.

Avnet Marshall: Business/IT Planning

Figure 14.5 outlines Avnet Marshall's planning process for business/IT initiatives and compares it with conventional IT planning approaches. Avnet Marshall weaves both business and IT strategic planning together *coadaptively* under the guidance of the CEO and the CIO, instead of developing IT strategy by just tracking and supporting business strategies. Avnet Marshall also locates IT application development projects within the business units that are involved in an e-business initiative to form centers of business/IT expertise throughout the company. Finally, Avnet Marshall uses a prototyping application development process with rapid deployment of new business applications instead of a traditional systems development approach. This application development strategy trades the risk of implementing incomplete applications with the benefits of gaining competitive advantages from early deployment of new e-business services to employees, customers, and other stakeholders and of involving them in the "fine-tuning" phase of application development.

Source: Adapted from Omar El Sawy, Arvind Malhotra, Sanjay Gosain, and Kerry Young, "IT-Intensive Value Innovation in the Electronic Economy: Insights from Marshall Industries," *MIS Quarterly*, September 1999.

Managing the IT Function

A radical shift is occurring in corporate computing—think of it as the recentralization of management. It's a step back toward the 1970s, when a data processing manager could sit at a console and track all the technology assets of the corporation. Then came the 1980s and early 1990s. Departments got their own PCs and software; client/server networks sprang up all across companies.

Three things have happened in the past few years: The Internet boom inspired businesses to connect all those networks; companies put on their intranets essential applications without which their businesses could not function; and it became apparent that maintaining PCs on a network is very, very expensive. Such changes create an urgent need for centralization.

Organizing IT

In the early years of computing, the development of large mainframe computers and telecommunications networks and terminals caused a **centralization** of computer hardware and software, databases, and information specialists at the corporate level of organizations. Next, the development of minicomputers and microcomputers accelerated a **downsizing** trend, which prompted a move back toward **decentralization** by many business firms. Distributed client/server networks at the corporate, department, workgroup, and team levels came into being, which promoted a shift of databases and information specialists to some departments and the creation of *information centers* to support end-user and workgroup computing.

Lately, the trend is to establish more centralized control over the management of the IT resources of a company while still serving the strategic needs of its business units, especially their e-business and e-commerce initiatives. This trend has resulted in the development of hybrid structures with both centralized and decentralized components. See Figure 14.6. For example, the IT function at Avnet Marshall is organized into several business-focused development groups, as well as operations management and planning groups.

Some companies spin off their information systems function into IS *subsidiaries* that offer IS services to external organizations, as well as to their parent company. Other companies create or spin off their e-commerce and Internet-related business units or IT groups into separate companies or business units. Corporations also **outsource,** that is, turn over all or parts of their IS operations to outside contractors known as *systems integrators*. In addition, some companies are outsourcing software procurement and support to *application service providers* (ASPs), which provide and support business application and other software via the Internet and intranets to all of a company's employee workstations. We will discuss outsourcing in greater detail later in this section. In the meantime, let's take a few minutes to review, and expand on, what we know about managing the various functions and activities in IS.

Managing Application Development

Application development management involves managing activities such as systems analysis and design, prototyping, applications programming, project management, quality assurance, and system maintenance for all major business/IT development projects. Managing application development requires managing the activities of teams of systems analysts, software developers, and other IS professionals working on a variety of information systems development projects. Thus, project management is a key IT management responsibility if business/IT projects are to be completed on time, within their budgets, and meet their design objectives. In addition, some systems

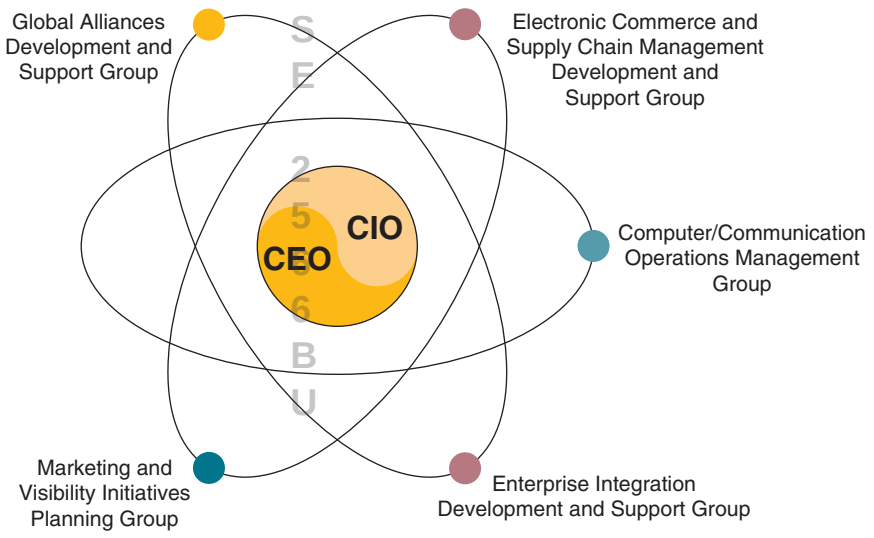


FIGURE 14.6
The organizational components of the IT function at Avnet Marshall.

development groups have established *development centers* staffed with IS professionals. Their role is to evaluate new application development tools and help information systems specialists use them to improve their application development efforts.

Managing IS Operations

IS operations management is concerned with the use of hardware, software, network, and personnel resources in the corporate or business unit **data centers** (computer centers) of an organization. Operational activities that must be managed include computer system operations, network management, production control, and production support.

Most operations management activities are being automated by the use of software packages for computer system performance management. These **system performance monitors** look after the processing of computer jobs, help develop a planned schedule of computer operations that can optimize computer system performance, and produce detailed statistics that are invaluable for effective planning and control of computing capacity. Such information evaluates computer system utilization, costs, and performance. This evaluation provides information for capacity planning, production planning and control, and hardware/software acquisition planning. It is also used in quality assurance programs, which emphasize the quality of services to business end users. See Figure 14.7.

System performance monitors also supply information needed by **chargeback systems** that allocate costs to users on the basis of the information services rendered. All costs incurred are recorded, reported, allocated, and charged back to specific end-user business units, depending on their use of system resources. When companies use this arrangement, the information services department becomes a service center whose costs are charged directly to business units rather than being lumped with other administrative service costs and treated as overhead costs.

Many performance monitors also feature **process control** capabilities. Such packages not only monitor but also automatically control computer operations at large data centers. Some use built-in expert system modules that are based on knowledge gleaned from experts in the operations of specific computer systems and operating systems. These performance monitors provide more efficient computer operations than human-operated systems. They also enable "lights out" data centers at some companies, where computer systems are operated unattended, especially after normal business hours.

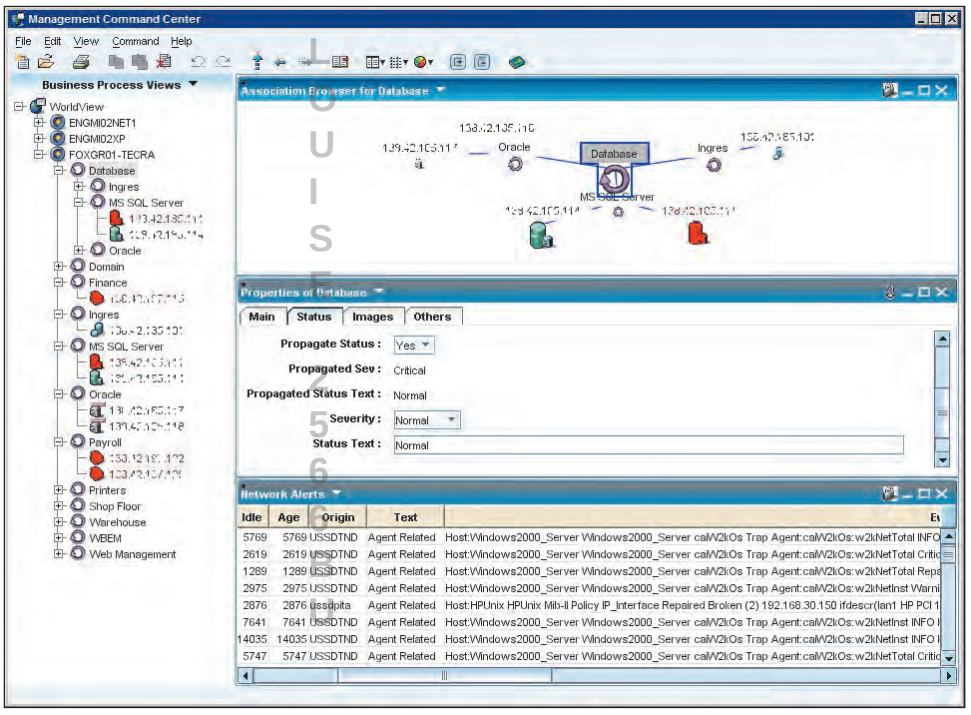


FIGURE 14.7
The CA-Unicenter TNG system performance monitor includes an Enterprise Management Portal module that helps IT specialists monitor and manage a variety of networked computer systems and operating systems.

Source: Courtesy of Computer Associates.

IT Staff Planning

The success or failure of an information services organization rests primarily on the quality of its people. Many firms consider **IT staff planning**, or recruiting, training, and retaining qualified IS personnel, as one of their greatest challenges. Managing information services functions involves the management of managerial, technical, and clerical personnel. One of the most important jobs of information services managers is to recruit qualified personnel and develop, organize, and direct the capabilities of existing personnel. Employees must be continually trained to keep up with the latest developments in a fast-moving and highly technical field. Employee job performances must be continually evaluated, and outstanding performances must be rewarded with salary increases or promotions. Salary and wage levels must be set, and career paths must be designed so that individuals can move to new jobs through promotion and transfer as they gain seniority and expertise.

The CIO and Other IT Executives

The **chief information officer (CIO)** oversees all use of information technology in many companies and brings it into alignment with strategic business goals. Thus, all traditional computer services, Internet technology, telecommunications network services, and other IS technology support services are the responsibility of this executive. The CIO does not direct day-to-day information services activities; instead, CIOs concentrate on business/IT planning and strategy. They also work with the CEO and other top executives to develop strategic uses of information technology in e-business and e-commerce that help make the firm more competitive in the marketplace. Many companies have also filled the CIO position with executives from the business functions or units outside the IS field. Such CIOs emphasize that the chief role of information technology is to help a company meet its strategic business objectives.

Top IT Jobs: Requirements and Compensation

- **Chief information officer**
  Base salary range: $194,000–$303,000+; varies by location
  Bonus range: Up to 40 percent of salary
  The top position in IT isn't all about technology. To land this job, you need to be a Business Technologist with a big "B" and a big "T." If you understand the business, the organization's strategy, and the broad spectrum of technologies, systems, applications, and people necessary to execute it, you will be in great demand by organizations.
- **Chief technology officer**
  Base salary range: $162,000–$245,000+; varies by location
  Bonus range: Up to 40 percent of salary
  If you're second-in-command to the CIO or chief technology officer and you have years of applications development experience, your next move should be into the chief technology officer's spot. To land this job, you'll need to be a passionate problem solver with a demonstrated record of reducing development time.
- **Chief security officer**
  Base salary range: $142,000–$205,000+; varies by location
  Bonus range: Up to 40 percent of salary
  If you understand the issues related to securing the data resources and information assets of the organization, then this is the job for you. Strong candidates with a deep understanding of both the technical and managerial sides of the field are in great demand.
- **E-commerce architect**
  Base salary range: $115,000–$170,000+; varies by location
  Bonus range: Up to 15 percent of salary
  If you know Java, Perl, C++, and Web services; have experience in systems architecture; and can design an Internet solution from concept through implementation, many companies want you to plan and develop their e-commerce sites.

- **Technical team leader**
  Base salary range: $75,000–$100,000+; varies by location
  Bonus range: Up to 20 percent of salary
  Senior technical team leaders with good communication, project management, and leadership skills, as well as knowledge of Web languages and databases, are still in great demand.
- **Practice manager**
  Base salary range: $70,000–$100,000+; varies by location
  Bonus range: Up to 20 percent of salary
  If you've got a background in IT assessment and a pedigree in business development (MBA preferred), you can land a job as a point person for big projects. You'll need skills in IT operations and software assessment, as well as in marketing, staffing, budgeting, and building customer relationships.
- **Systems analyst**
  Base salary range: $56,000–$100,000+; varies by location
  Bonus range: Up to 25 percent of salary
  If you have problem-solving skills and a degree in information systems (BS or MBA), you can be assured of finding a good job as a systems analyst. You'll need to have excellent interpersonal skills, good technical skills, and an ability to apply your problem-solving and critical-thinking skills to the design of new systems.

Source: www.salary.com.

Technology Management

The management of rapidly changing technology is important to any organization. Changes in information technology, like the rise of the PC, client/server networks, and the Internet and intranets, have come swiftly and dramatically and are expected to continue into the future. Developments in information systems technology have had, and will continue to have, a major impact on the operations, costs, management work environment, and competitive position of many organizations.

Thus, all information technologies must be managed as a technology platform for integrating internally focused or externally facing business applications. Such technologies include the Internet, intranets, and a variety of e-commerce and collaboration technologies, as well as integrated enterprise software for customer relationship management, enterprise resource planning, and supply chain management. In many companies, **technology management** is the primary responsibility of a **chief technology officer (CTO)**, who is in charge of all information technology planning and deployment.

Managing User Services

Teams and workgroups of business professionals commonly use PC workstations, software packages, and the Internet, intranets, and other networks to develop and apply information technology to their work activities. Thus, many companies have responded by creating **user services**, or *client services*, functions to support and manage end-user and workgroup computing.

End-user services provide both opportunities and problems for business unit managers. For example, some firms create an *information center* group staffed with user liaison specialists or Web-enabled intranet help desks. IS specialists with titles such as user consultant, account executive, or business analyst may also be assigned to end-user workgroups. These specialists perform a vital role by troubleshooting problems, gathering and communicating information, coordinating educational efforts, and helping business professionals with application development.

In addition to these measures, most organizations still establish and enforce policies for the acquisition of hardware and software by end users and business units. This process ensures their compatibility with company standards for hardware, software,

and network connectivity. Also important is the development of applications with proper security and quality controls to promote correct performance and safeguard the integrity of corporate and departmental networks and databases.

Outsourcing and Offshoring IT and IS

An increasingly popular approach to managing the IS and IT functions of the organization is to adopt an outsourcing strategy. **Outsourcing**, in broad terms, is the purchase of goods or services that were previously provided internally from third-party partners. Outsourcing is a generic term used for a broad range of information technology functions that are selectively contracted to an external service provider.

Outsourcing

A commonly outsourced IS function is software application development. This process includes contracting (or subcontracting) with an external organization for the development of complete or partial software products/projects, the purchase of packaged or customized package software products, or activities and/or resources that aid in the software development life cycle. Figure 14.8 lists the functions typically outsourced, the reasons behind the decision to outsource, and several aspects associated with successful vendor selection and a successful outsourcing effort.

Although companies can, theoretically, choose to outsource any organization function for any reason, there are five main reasons behind a decision to outsource:

FIGURE 14.8 Outsourcing's Top 10. Notice, despite all of the media coverage, application development is No. 3.

Top 10 Reasons Companies Outsource	Top 10 Factors in Vendor Selection
1. Reduce and control operating costs	1. Commitment to quality
2. Improve company focus	2. Price
3. Gain access to world-class capabilities	3. References/reputation
4. Free internal resources for other purposes	4. Flexible contract terms
5. Necessary resources are not available internally	5. Scope of resources
6. Accelerate reengineering benefits	6. Additional value-added capability
7. Function is difficult to manage internally or is out of control	7. Cultural match
8. Make capital funds available	8. Existing relationship
9. Share risks	9. Location
10. Cash infusion	10. Other
Top 10 Factors for Successful Outsourcing	**Top 10 IT Areas Being Outsourced**
1. Understand company goals and objectives	1. Maintenance and repair
2. A strategic vision and plan	2. Training
3. Select the right vendor	3. Applications development
4. Ongoing management of the relationships	4. Consulting and reengineering
5. A properly structured contract	5. Mainframe data centers
6. Open communication with affected individuals/groups	6. Client/server services and administration
7. Senior executive support and involvement	7. Network administration
8. Careful attention to personnel issues	8. Desktop services
9. Near-term financial justification	9. End-user support
10. Use of outside expertise	10. Total IT outsourcing

Source: The Outsourcing Institute.

Save Money—Achieve Greater Return on Investment (ROI)

- Outsourcing IS/IT functions to skilled service providers is often a strategic approach to stretching strained budgets. Companies that take a well-managed approach to outsourcing can gain cost savings of upwards of 40–80 percent.

Focus on Core Competencies

- Outsourced professionals allow an organization and its employees to focus on the business they are in rather than a business in which they are not. By using an outsourcing strategy for application development, an organization can focus its IS professionals on identifying and solving business problems rather than on programming and prototyping new applications.

Achieve Flexible Staffing Levels

- Strategic use of an outsourcing approach to IS/IT functions can result in business growth without increasing overhead. Outsourcing provides a pool of qualified professionals available for unique, niche, or overflow projects. If the unique skill set required by an organization is difficult to find or expensive to maintain in-house, outsourcing can allow for the acquisition of the needed expertise.

Gain Access to Global Resources

- The Outsourcing Institute asserts that the rules for successfully growing a business have changed: "It's no longer about what you own or build. . . . [Instead] success is hinged to resources and talent you can access." Using global expertise allows an organization to gain the advantage of skilled labor, regardless of location, and significantly increase the quality of its deliverables. As such, outsourcing can create opportunities for smaller businesses that might not otherwise be possible due to costs or geophysical constraints.

Decrease Time to Market

- Outsourcing extends the traditional small business benefits of flexibility and responsiveness, allowing smaller organizations to compete effectively against bigger firms. Supplementing an existing workforce with offshore support could allow for productivity 24 hours a day. Having access to resources able to work on key projects even while local employees are asleep can serve to accelerate time to market and provide a key competitive advantage.

Offshoring

Although often confused with outsourcing, offshoring is also increasingly becoming part of a strategic approach to IS/IT management. **Offshoring** can be defined as a relocation of an organization's business processes (including production/manufacturing) to a lower-cost location, usually overseas. Offshoring can be considered in the context of either *production* offshoring or *services* offshoring. After its accession to the World Trade Organization (WTO), China emerged as a prominent destination for production offshoring. After technical progress in telecommunications improved the possibilities of trade in services, India became a country that chose to focus on this domain.

The growth of services offshoring in information systems is linked to the availability of large amounts of reliable and affordable communication infrastructure following the telecom bust of the late 1990s. Coupled with the digitization of many services, it became possible to shift the actual delivery location of services to low-cost locations in a manner theoretically transparent to end users.

India, the Philippines, Ireland, and Eastern European countries benefited greatly from this trend due to their large pool of English-speaking and technically qualified workers. India's offshoring industry took root in IT functions in the 1990s and has since moved to back-office processes, such as call centers and transaction processing, as well as high-end jobs such as application development.

Offshoring is often enabled by the transfer of valuable information to the offshore site. Such information and training allows the remote workers to produce results of comparable value previously produced by internal employees. When such transfer includes proprietary materials, such as confidential documents and trade secrets, protected by nondisclosure agreements, then intellectual property has been transferred or exported. The documentation and valuation of such exports is quite difficult but should be considered because it comprises items that may be regulated or taxable.

Offshoring has been a controversial issue with heated debates. On one hand, it is seen as benefiting both the origin and destination country through free trade. On the other hand, job losses in developed countries have sparked opposition to offshoring. Some critics agree that both sides will benefit in terms of overall production and numbers of jobs created but that the subjective quality of the new jobs will be less than the previous ones. While this debate continues, companies continue to use offshoring as a viable IS/IT management approach. Let's look at a real-world example of global outsourcing.

Royal Dutch Shell: Multisupplier Global Outsourcing Deal

Royal Dutch Shell has signed a five-year, $4 billion outsourcing deal with three global IT and telecommunications suppliers. The value of the contracts for the three suppliers is $1.6 billion with AT&T, $1 billion for EDS, and $1.6 billion with T-Systems.

Shell announced that it has contracted T-Systems, AT&T, and EDS under a master service agreement (MSA), for "significant improvements" to its efficiency and productivity that will see an axing of some tech jobs and a transfer of 3,000 IT staff to the service providers. Under the MSA, Shell will outsource its IT infrastructure in three service bundles: "AT&T for network and telecommunications, T-Systems for hosting and storage, and EDS for end user computing services and for integration of the infrastructure services."

The suppliers will provide integrated services to more than 1,500 sites worldwide. "Shell's approach combines all the advantages of decentralised service provision with the benefits and efficiency of a centralised governance structure," says Elesh Khakhar, a partner at consultant firm TPI, which is an advisor to Shell. Khakar added that the multisupplier deal has been designed to "encourage collaborative behavior" between suppliers, while it allows Shell to "retain full control of strategy and service integration. In addition to all of the usual business benefits, Shell will be able to exploit emerging commoditized services designed for the consumer market, such as email or internet phone services, and integrate them within their services when they become robust enough for commercial use."

Shell CIO Alan Matula said: "This deal is a major strategic choice for Shell. Partnering with EDS, T-Systems and AT&T gives us greater ability to respond to the growing demands of our businesses. It allows Shell IT to focus on Information Technology that drives competitive position in the oil and gas market, whilst suppliers focus on improving essential IT capability."

Source: Adapted from Siobhan Chapman, "Shell Signs $4 Billion, Multi-Supplier Outsourcing Deal," *CIO Magazine*, April 3, 2008.

Trends in Outsourcing and Offshoring

While in the past much of the motivation to outsource and offshore various portions of the IT/IS operation of a firm were driven primarily by cost, a more recent and troubling trend is the increasing motivation to find highly qualified IT/IS talent. Jobs are plentiful in the United States for today's IS graduate, but enrollments in United States's IS programs remain down. This results in a decreasing supply of qualified labor for the best paying jobs in the field. To combat this, firms are looking at the science and

engineering graduate of other countries to fill their needs. As we discussed in Chapter 2, the jobs that were outsourced and offshored in the late 1990s and early 2000 were not the ones typically benchmarked by university-level IS programs. As such, no real job opportunities were lost to qualified graduates. Today, however, the lack of qualified IS graduates means companies have to turn elsewhere to fill these jobs. The jobs are staying here, but the labor is being imported. The single most effective method to counter this trend is for more young people to seek a career in the information systems field. IS/IT is one of the hottest fields on the planet for job opportunities, and the word needs to get out. Many organizations are focusing on outreach programs that extend down to the pre-high school levels to begin educating, or reeducating, the public with regard to these vast opportunities.

Failures in IT Management

Managing information technology is not an easy task. The information systems function often has performance problems in many organizations. The promised benefits of information technology have not occurred in many documented cases. Studies by management consulting firms and university researchers have shown that many businesses have not been successful in managing their use of information technology. Thus, it is evident that in many organizations, information technology is not being used effectively and efficiently, and there have been **failures in IT management.** For example:

- Information technology is not being used *effectively* by companies that use IT primarily to computerize traditional business processes instead of developing innovative e-business processes involving customers, suppliers, and other business partners, e-commerce, and Web-enabled decision support.
- Information technology is not being used *efficiently* by information systems that provide poor response times and frequent downtimes, or by IS professionals and consultants who do not properly manage application development projects.

Let's look more closely, using a real-world example.

Risk without Reward: Weak IT Controls at Société Générale

It's a lethal combination of process oversights and system failures that is the stuff of CIO nightmares: An investigation into rogue trader Jerome Kerviel's fraudulent actions at Société Générale bank uncovered an apparent breakdown in financial and internal IT controls, subverted by an employee with IT know-how and authorized systems access. IT experts say the case should serve as a warning that businesses can do better to manage IT-related risk.

"Much time is spent on protecting the external threat," says J.R. Reagan, managing director and global solution leader for risk, compliance and security at BearingPoint. "But the internal threat can be even larger in terms of risk to the company." In the case of Société Générale, not only were IT security controls insufficient, but the bank's staff did not fully investigate red flags that arose. Recent research by the Ponemon Institute concludes that "insider threats represent one of the most significant information security risks." In a survey of 700 IT practitioners, 78 percent said they believe individuals have too much access to information that isn't pertinent to their jobs, while 59 percent said such access presents business risks. What's more, IT professionals see a disconnect with business leaders: 74 percent said senior management does not view governance of access to information as a strategic issue.

One of Société Générale's primary business lines is derivatives—financial instruments that allow traders to make contracts on a wide range of assets (such as equities, bonds, or commodities) and attempts to reduce (or hedge) the financial risk for one party in the deal. Trading derivatives, however, necessitates some aggressiveness and can be fraught with risk.

Reagan observes that in the case of Société Générale, "their activities deal with high volume, high velocity and quick tempo trading of stock," and it's likely business leaders "wouldn't put up with" security measures that would slow them down. For example, Société Générale employed single-factor authentication (using one method, such as passwords, to grant access to its systems) rather than stronger dual-factor authentication (requiring that individuals employ two methods of identifying themselves to gain access). "The security team needs to explain the risk exposure and the possibility of losing billions in fraudulent trades if security is not adequately addressed," Reagan says. "But most security guys aren't well enough in tune with the business to be able to articulate a business case like that."

That disconnect can be enormously destructive, as the Société Générale incident shows. "The Société Générale case brings to the fore the fact that business risk can be directly exposed through IT," says Scott Crawford, a security expert and research director at Enterprise Management Associates. "Kerviel allegedly manipulated the IT controls on the business systems based on his midoffice experience and back-office knowledge and expertise."

"Businesses are just now beginning to awaken to the controls within the IT environment," Crawford says. "If you're betting the farm and strategy on the IT controls, it behooves the organization to ensure that those controls are reasonably resistant to subversion."

Source: Adapted from Nancy Weil, "Risk without Reward," *CIO Magazine*, May 1, 2008.

Management Involvement

What is the solution to failures in the information systems function? There are no quick and easy answers. However, the experiences of successful organizations reveal that extensive and meaningful **managerial and end-user involvement** is the key ingredient of high-quality information systems performance. Involving business managers in the governance of the IS function and business professionals in the development of IS applications should thus shape the response of management to the challenge of improving the business value of information technology. See Figure 14.9.

Involving managers in the management of IT (from the CEO to the managers of business units) requires the development of *governance structures* (e.g., executive councils, steering committees) that encourage their active participation in planning and controlling the business uses of IT. Thus, many organizations have policies that require managers to be involved in IT decisions that affect their business units. This requirement helps managers avoid IS performance problems in their business units and development projects. With this high degree of involvement, managers can improve the strategic business value of information technology. Also, as we noted in Chapter 12, only direct end-user participation in system development projects can solve the problems of employee resistance and poor user interface design. Overseeing such involvement is another vital management task.

IT Governance

Information technology governance (ITG) is a subset discipline of corporate governance focused on the information technologies (IT), information systems (IS), their performance, use, and associated risks. The rising interest in IT governance is due, in part, to governmental compliance initiatives such as Sarbanes-Oxley in the United States and its counterpart in Europe, Basel II. Additional motivation comes from the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization.

A characteristic theme of IT governance discussions is that the IT capability can no longer be thought of as a mythical black box, the contents of which are known only to the IT personnel. This traditional handling of IT management by board-level executives is due to limited technical experience and the perceived complexity of IT. Historically, key

FIGURE 14.9 Senior management needs to be involved in critical business/IT decisions to optimize the business value and performance of the IT function.

IT Decision	Senior Management's Role	Consequences of Abdicating the Decision
• **How much should we spend on IT?**	Define the strategic role that IT will play in the company, and then determine the level of funding needed to achieve that objective.	The company fails to develop an IT platform that furthers its strategy, despite high IT spending.
• **Which business processes should receive our IT dollars?**	Make clear decisions about which IT initiatives will and will not be funded.	A lack of focus overwhelms the IT unit, which tries to deliver many projects that may have little companywide value or can't be implemented well simultaneously.
• **Which IT capabilities need to be companywide?**	Decide which IT capabilities should be provided centrally and which should be developed by individual businesses.	Excessive technical and process standardization limit the flexibility of business units, or frequent exceptions to the standards increase costs and limit business synergies.
• **How good do our IT services really need to be?**	Decide which features—for example, enhanced reliability or response time—are needed on the basis of their costs and benefits.	The company may pay for service options that, given its priorities, aren't worth their costs.
• **What security and privacy risks will we accept?**	Lead the decision making on the trade-offs between security and privacy on one hand and convenience on the other.	An overemphasis on security and privacy may inconvenience customers, employees, and suppliers; an underemphasis may make data vulnerable.
• **Whom do we blame if an IT initiative fails?**	Assign a business executive to be accountable for every IT project; monitor business metrics.	The business value of systems is never realized.

Source: Jeanne W. Ross and Peter Weill, "Six IT Decisions Your IT People Shouldn't Make," *Harvard Business Review*, November 2002, p. 87.

decisions were often deferred to IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers, and related areas such as finance, have the necessary input into the decision-making process. This prevents a single stakeholder, typically IT, from being blamed for poor decisions. It also prevents users from later complaining that the system does not behave or perform as expected.

The focus of ITG is specifying decision inputs and rights along with an accountability framework such that desirable behaviors toward and in the use of IT are developed. It highlights the importance of IT-related matters in contemporary organizations and ensures that strategic IT decisions are owned by the corporate board, rather than by the CIO or other IT managers. The primary goals for information technology governance are to (1) assure that the significant organizational investments in IT and IS generate their maximum business value and (2) mitigate the risks that are associated with IT. This is accomplished by implementing an organizational structure with well-defined roles for the responsibility of the decisions related to the management and use of IT such as infrastructure, architecture, investment, and use.

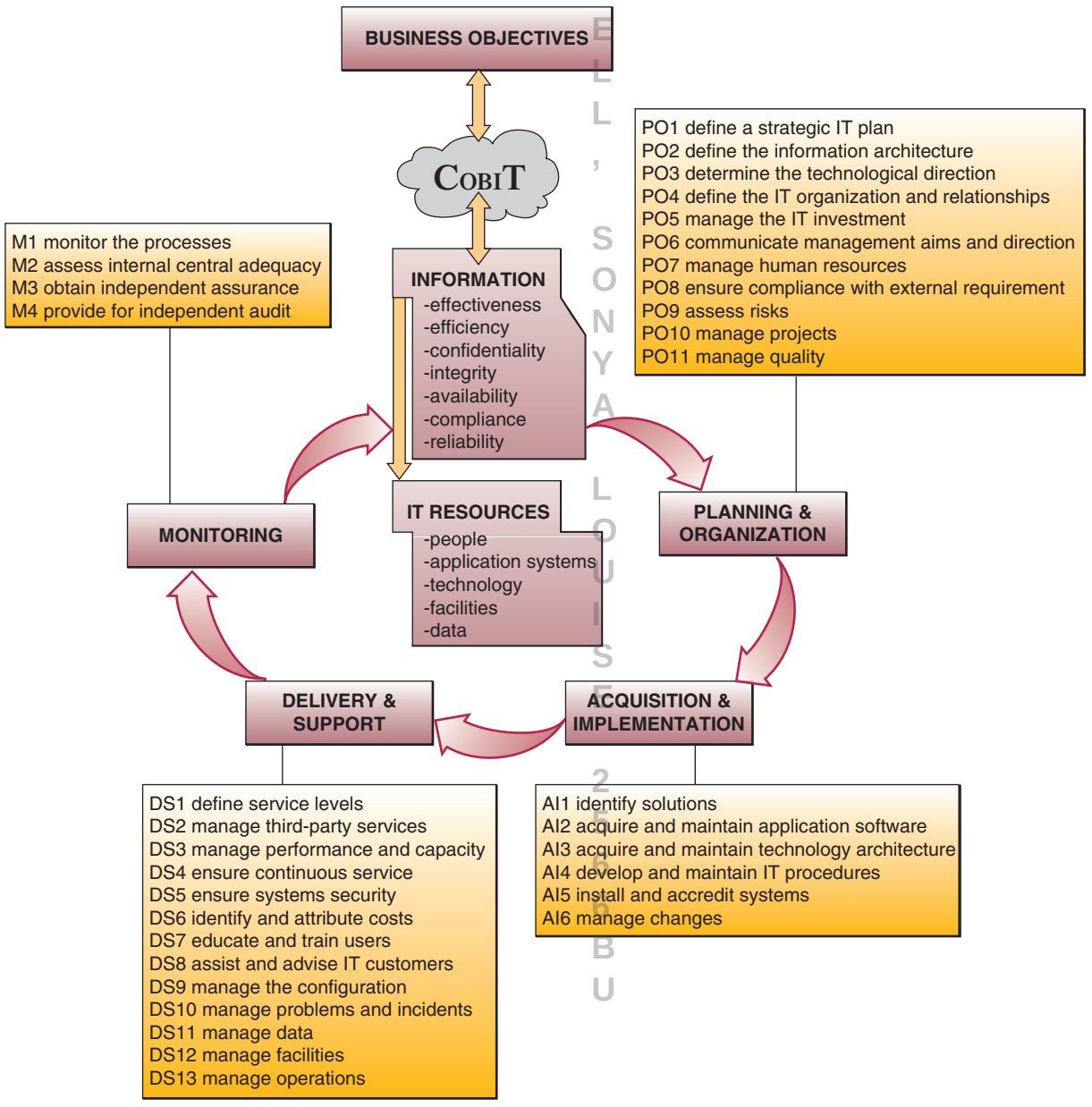
One very popular approach to IT governance is COBIT (Control Objectives for Information and related Technology). COBIT is a framework of best practices for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT provides all members of the organization with a set of generally accepted measures, indicators, processes, and best practices to help them maximize the benefits derived through the use of information technology and in developing appropriate IT governance and control structures in a company.

COBIT has 34 high-level processes covering 210 control objectives categorized in four domains: (1) Planning and Organization, (2) Acquisition and Implementation,

(3) Delivery and Support, and (4) Monitoring. Managers benefit from COBIT because it provides them with a foundation upon which IT-related decisions and investments can be based. Decision making is more effective because COBIT helps management define a strategic IT plan, define the information architecture, acquire the necessary IT hardware and software to execute an IT strategy, ensure continuous service, and monitor the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them by COBIT's defined controls, security, and process governance. COBIT also benefits auditors because it helps them identify IT control issues within a company's IT infrastructure, and it helps them corroborate their audit findings. Figure 14.10 illustrates the relationships between the four domains in COBIT and categorizes both the high-level processes and control objectives associated with them.

Let's look at a real-world example of COBIT in action.

FIGURE 14.10 COBIT is a popular IT governance approach that focuses on all aspects of the IT function throughout the organization.



Blue Cross and Blue Shield of North Carolina: Reaping Benefits from a Successful COBIT Implementation

Blue Cross and Blue Shield of North Carolina is a leading health services company that delivers quality products, information, and services to help its customers improve their health and well-being.

In 2004, external audit firms raised the bar on the level of IT controls because of the U.S. Sarbanes-Oxley Act of 2002. In response, Blue Cross and Blue Shield of North Carolina, USA (BCBSNC), created a remediation program that addressed each Sarbanes-Oxley-related issue individually.

In 2006, BCBSNC began preparing for the National Association of Insurance Commissioners's (NAIC) Sarbanes-Oxley–like compliance requirements, called the Model Audit Rule.

Because of the team's research into and selection of the COBIT IT governance framework, BCBSNC was aware that COBIT could also be leveraged to meet Sarbanes-Oxley compliance requirements.

BCBSNC used a couple of unique requirements to help provide focus and set priorities. First, the financially significant applications had to be addressed. The second requirement was called "COBIT Lite." The team used the financially significant applications to narrow the scope of what they looked at and self-tested. For example, when the team looked at backup and recovery, they only looked at the platforms that housed the financially significant applications.

"COBIT Lite" referred to the pragmatic approach the team adopted. The work was performed by employees in addition to their day jobs so they focused on reasonable and prudent controls for the environment.

BCBSNC received numerous benefits from implementing the COBIT framework. Notable benefits include formalizing and documenting controls policies and procedures. For the most part, the required controls were in place when they set off on this odyssey; however, little was documented, and procedures were informal.

Many areas achieved benefits from the self-testing program, including noticing minor exceptions right away and being able to correct them before they became any larger. The team also found that it could use COBIT as a common language, which worked internally among various process areas, as well as with internal auditors.

Any undertaking of this size has some great lessons. It is best to build the controls into the process. It makes the controls easier to sustain and it makes self-testing more efficient and effective. If the controls are not built into the process, the area performing the self test may have to pull and review a quarter's worth of documentation. This can take numerous hours. If the control point is built into the process as a quality assurance step, self-testing is always done; they just have to submit the documentation/evidence.

Enterprises should also limit the number of processes they attempt to implement at one time. BCBSNC took on 14 partial processes, and it took them *two and a half years* to get everything in place and operating. And that was without encountering any major roadblocks.

Source: Adapted from Marty King, "COBIT Case Study: Blue Cross and Blue Shield of North Carolina," *ISACA Case Studies*.

SECTION II Managing Global IT

The International Dimension

Whether they are in Berlin or Bombay, Kuala Lumpur or Kansas, San Francisco or Seoul, companies around the globe are developing new models to operate competitively in a digital economy. These models are structured, yet agile; global, yet local; and they concentrate on maximizing the risk-adjusted return from both knowledge and technology assets.

International dimensions have become a vital part of managing a business enterprise in the inter-networked global economies and markets of today. Whether you become a manager in a large corporation or the owner of a small business, you will be affected by international business developments and deal in some way with people, products, or services whose origin is not your home country.

Read the Real World Case on the next page. We can learn a lot about the challenges facing senior IT executives who operate in a globalized world. See Figure 14.11.

Global IT Management

Figure 14.12 illustrates the major dimensions of the job of managing global information technology that we cover in this section. Notice that all global IT activities must be adjusted to take into account the cultural, political, and geoeconomic challenges that exist in the international business community. Developing appropriate business and IT strategies for the global marketplace should be the first step in **global information technology management**. Once that is done, end users and IS managers can move on to developing the portfolio of business applications needed to support business/IT strategies; the hardware, software, and Internet-based technology platforms to support those applications; the data resource management methods to provide necessary databases; and finally the systems development projects that will produce the global information systems required.

Global Teams: It's Still a Small World

We seem to have reached a point where virtually every CIO is a global CIO—a leader whose sphere of influence (and headaches) spans continents. The global CIO's most common challenge, according to CIO Executive Council members, is managing global virtual teams. In an ideal world, HR policies across the global IT team should be consistent, fair, and responsive. Titles and reporting structures (if not compensation) should be equalized.

The council's European members, representing Royal Dutch Shell, Galderma, Olympus, and others, commissioned a globalization playbook that collects and codifies best practices in this and other globalization challenges.

Obtain local HR expertise. Companies must have a local HR person in each country to deal with local laws. "Hiring, firing, and training obligations must be managed very differently in each location, and you need someone with local expertise on the laws and processes," says Michael Pilkington, former chief information officer of Euroclear, the Brussels-based provider of domestic and cross-border settlement for bond, equity, and fund transactions.

Create job grade consistency across regions. Euroclear is moving toward a job evaluation methodology that organizes job types into vertical categories, such as managing people/process, product development, business support, and project management. This provides a basis for comparing and managing roles and people across locations. Grade level is not the same thing as a title; people's titles are much more subject to local conventions.

(text continues on page 601)

REAL WORLD CASE 2

Cadbury, Forrester Research, A.T. Kearney, and Others: IT Leaders Face New Challenges in a Globalized World

Wayne Shurts had no experience overseeing IT operations in emerging markets when Cadbury CEO Todd Stitzer appointed him global CIO the summer of 2009. The geographic parameters of Shurts's responsibilities at the sweets maker—with a presence everywhere from Pakistan to Palau—multiplied overnight. The former CIO for North America now spends most of his time globe-trotting from his home base in Parsippany, New Jersey, to London headquarters to operations on six continents.

Shurts also had to shift his thinking. The $7.8 billion company has made a concerted effort to expand in the developing world, giving it the biggest and most dispersed emerging markets business in the confectionery industry. In fact, Cadbury's business in rapidly developing markets was a major driver in Kraft's $19.5 billion takeover bid for the British candy maker. Last year, 60 percent of the company's growth came from emerging markets.

"That means that my world as CIO does not solely revolve around big economies of North America, Europe, Australia and New Zealand," explains Shurts.

"Emerging markets are not afterthoughts to me. They demand—and get—a lot of my attention." Shurts isn't alone. In industries ranging from consumer goods and agriculture to banking and electronics, multinationals are investing more in the Middle East, Asia, Eastern Europe, Africa, and South America. Now imagine developing a single system that manages reinsurance business processes for numerous offices around the world—offices whose staffs speak different languages, are in different time zones, and just might be stuck in their ways as to how they manage their business. It's a challenge that could overwhelm you if you tried to tackle it all at once instead of breaking it into small pieces.

"Companies are going to tap those markets as mature markets stagnate or decline," says Bob Haas, a partner and vice president with A.T. Kearney who leads the consultancy's strategic IT practice for North America. "And CIOs are gaining more and more responsibility for those emerging markets since IT is one of the most globally integrated corporate functions."

The work amounts to much more than just bringing some distant locations into the IT fold. Setting up shop in Bogotá or in Bursa, Turkey, is clearly a different proposition than supporting a new office in Boise, Idaho, or Brussels. Infrastructure limitations, local talent supply, unfamiliar business and cultural norms, limited vendor support, and restricted budgets require creative solutions. At the same time, there is pressure to integrate these often one-off extensions of the company into the global infrastructure.

Bobby Cameron, vice president and principal analyst with Forrester Research, got a call recently from the chief information officer of a U.S.-based agribusiness building a new manufacturing plant in a tiny Peruvian fishing village. "It's 250 miles away from Lima. There's no water. There's no electricity. There's nothing there," Cameron says. "What's that about?"

It's about having an ideal port for moving goods throughout South America. All the chief information officer has to do is figure out how to build something from nothing without many of the support structures—vendors, a trained workforce, infrastructure—he'd have in a mature market. "And once you get through all of that," says Cameron," then you have to figure out how to connect it to the global infrastructure."

It's an extreme example, but supporting business in developing regions rarely lends itself to cookie-cutter IT. Moreover, the importance of emerging markets today means IT leaders can't fob off secondhand technology to non-Western locations.

"The strategy of many corporations was basically to develop things in major markets then hand down those solutions to the emerging markets," Shurts says. "Hey, this laptop is two years old, maybe we pass that down, too."

That's not the case at Cadbury, explains Shurts. "I have to deliver strategies that address the specific needs of emerging markets. It requires some creativity and new thinking."

Understanding your company's business model for developing markets is critical. "Will there be manufacturing? Will you distribute from this market? How will your salesforce engage customers and what is their role while engaged?" says Ed Holmes, vice president of Global IT for Stiefel, an $812 million dollar skin care company, acquired by GlaxoSmithKline, that operates in 28 countries.

You may end up providing technology and services similar to those you supply in established markets, Holmes adds, "but you must challenge the baseline assumptions in order to ensure that your solution will fit the market both economically and culturally."

FIGURE 14.11

Emerging economies are increasingly demanding—and getting—IT executives' attention.

Source: © Getty Images.

LUTTRELL, SONYA LOUISE 256 6BU

Obstacles vary by location. Many developing markets face disadvantages after decades of having closed economies, including limited exposure to global business practices. But two overriding—and sometimes conflicting—considerations for global CIOs are cost structure and scalability. "From an IT perspective, these markets need to grow at an investment rate that makes sense for them," Shurts explains. "What they need today may not be what they need tomorrow. And tomorrow might actually mean tomorrow."

In its early days, an operation in an emerging market country may not need, nor could it support, the complexity and cost of a full-fledged ERP system. "Then, suddenly, through organic growth and an acquisition, everything changes and you do need the disciplines and features that an ERP system provides," Shurts says.

For instance, there's little support for emerging market needs among IT vendors, which means global CIOs and their teams go it alone, for the most part. Traditional solutions from IT vendors can be "too heavy and expensive for emerging markets," says Shurts. "It is very easy and neat and comfortable to walk around with that developed market mind-set. There's a whole industry of people who would love for you to do that—hardware, software companies that have built their businesses focused on the developed market," Shurts says. "It's much harder to get out of that comfort zone."

Typical of global CIOs, Shurts finds that exciting. "Many of them enjoy starting from scratch," says Forrester's Cameron. "They can't turn to IBM or SAP and have them solve all of their problems."

Cadbury does try to take advantage of corporate-level IT investments where possible. "We can leverage some systems from our developed markets and adapt that to emerging markets at a much lower cost," Shurts says.

SAP instances, for example, where 80 percent of the investment has been made in a more established market, may be used in a developing market, even if that new market can't support all the same capabilities, has different legal or regulatory needs, or requires unique functionality. The Australia instance has been leveraged in parts of Asia; the Britain/Ireland instance has been reused in South Africa; and the initial instance in Brazil is being recycled for use throughout Latin America.

Other IT priorities just don't apply. In the United States, Canada, and Australia, Cadbury IT is laser-focused on trade promotion management. Sophisticated tools are used to analyze the amount of money Cadbury spends and types of corporate programs it uses to promote its products.

None of that will do a lick of good in South America or India, where the mom-and-pop shop still rules, and there are no big promotions to manage with Wal-Mart. Rather, the focus is on lower-end tools to determine the right delivery routes, make sales calls, and take orders. The good news is that there are similarities across the company's locations. "Route-to-market tools, salesforce automation and supply chain planning are important to all emerging markets," Shurts says.

Every country has its own particular problems. In some, the concept of urgency—embedded in the workplace culture of established markets—is foreign. In others, it is about infrastructure, or lack thereof. For instance, notes Shurts, most countries in Africa still struggle with broadband access. This problem will be alleviated somewhat by submarine cable projects on either side of the continent, scheduled to go live this fall, but "that's the most frustrating thing for us," Shurts says. "We do a lot of satellite in Africa and with our global applications—HR, finance. You'll notice slower response rates and latency."

Importing hardware and software may be the best way to go in Dubai and Abu Dhabi. But CIOs managing IT in Brazil—including Shurts and Holmes—know that heavy tariffs there mean it's cheaper to buy everything in-country. "Our standard procurement solution doesn't really work there," says Holmes. "The only way you learn about these country-specific challenges is by engaging with other CIOs, talking to your HR leads in those locations and paying attention to previous challenges in other business functions."

"You have the ability to completely rethink the norms. This lets you create new solutions that would not have otherwise been viable," says Holmes. "The best opportunity is learning something that can then be translated back to a larger, more costly country." Less-developed regions of the world can also serve as testing grounds for new technologies or processes, says Haas, because the IT environment is less complex.

It's a big job, but lots of CIOs are going to have to do it, says Haas, who thinks developing markets experience is becoming a rite of passage for tomorrow's multinational CIOs. "Because we're a business with a very big presence in emerging markets, I am faced with the challenges of supporting IT in developing markets more than my peers," says Shurts. "But for others, it's coming. It's absolutely coming."

Source: Adapted from Stephanie Overby, "Globalization: New Management Challenges Facing IT leaders," *CIO.com*, November 12, 2009.

CASE STUDY QUESTIONS

1. What are the challenges faced by the CIOs mentioned in the case? Group them into categories and use examples from the case to define each.
2. The case mentions that the traditional approach toward emerging countries had been to develop technology in the corporate offices and then hand them down to satellite operations. How has that changed, as discussed in the case?
3. "IT is one of the most globally integrated corporate functions." How is IT different from other business areas when it comes to global integration? Why do you think this is the case?

REAL WORLD ACTIVITIES

1. Go online and search for other examples of large multinational organizations facing similar challenges. Summarize your findings and compare them to the ones chronicled in the case. Can you find any new ones not mentioned here?
2. Do you think some form of international experience is key to your long-term career success? Have you ever considered taking a position abroad? Why or why not? Break into small groups with your classmates to discuss the advantages and disadvantages of moving abroad to gain these experiences.

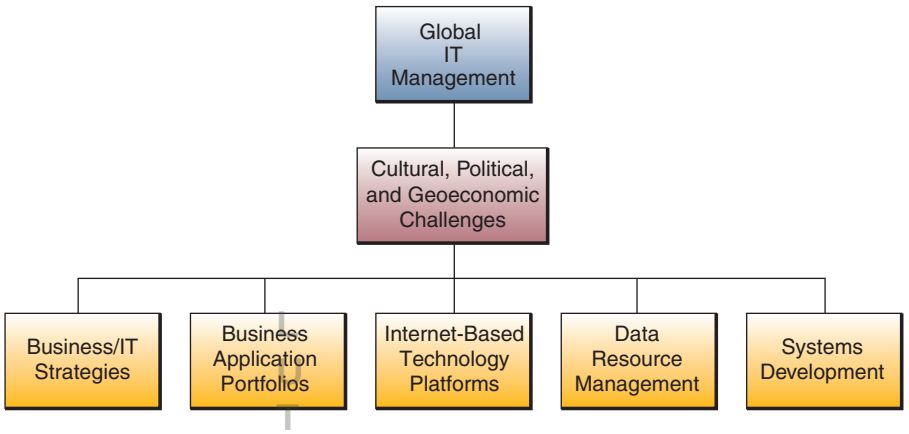


FIGURE 14.12
The major dimensions of global e-business technology management.

Manage dispersed staff as portfolio teams. ON Semiconductor has IT staff that support sales in Slovakia, where ON has a factory; in Hong Kong, where ON has a major sales office; in Shenzhen, China, where a customer service center is located; and in Kuala Lumpur, Malaysia, at its regional development center. ON overcomes potential disconnects by having a single sales IT portfolio owner, based at headquarters in Phoenix, who sets objectives and distributes work to the members of that team no matter where they reside.

Make the work meaningful. To keep morale high and turnover low, be sure that each remote location contributes to important projects. Don't send remote workers a steady diet of maintenance. Pilkington suggests building a center of excellence in each remote location.

Clearly defining the roles of remote groups can also help knit them together. For example, global company leaders can hold meetings at all levels to discuss the distinct purposes of corporate headquarters, the regions, and the local units. Knowing what their roles are in the larger picture and what they can expect from others "creates a sense of identity and purpose," says Nariman Karimi, senior vice president and chief information officer of DHL Asia Pacific.

Bring remote staff to headquarters. ON Semiconductor brings its foreign-based employees to the United States to work on key initiatives and interact with other business units at corporate headquarters. This may not be a monetary reward, but in many cultures it represents an endorsement and source of pride.

Foster communication across regional boundaries. Videoconferencing is an obvious tool to enhance global team communication, but it's important to have in-person meetings as well. At DHL, Karimi, together with the regional board members, visits one of the top 10 sites around the Asia Pacific region each month; each gets at least one personal visit a year. The visits include time for the local unit to showcase itself, and there is also unstructured time for informal and personal interaction.

Source: Adapted from Richard Pastore, "Global Team Management: It's a Small World After All," *CIO Magazine*, January 23, 2008.

Cultural, Political, and Geoeconomic Challenges

"Business as usual" is not good enough in global business operations. The same holds true for global e-business technology management. There are too many cultural, political, and geoeconomic (geographic and economic) realities that must be confronted for a business to succeed in global markets. As we have just mentioned, global information technology management must focus on developing global business IT strategies and managing global e-business application portfolios, Internet technologies, platforms, databases, and systems development projects. Managers, however, must

also accomplish this task from a perspective and through methods that take into account the cultural, political, and geoeconomic differences that exist when doing business internationally.

For example, a major **political challenge** is that many countries have rules regulating or prohibiting transfer of data across their national boundaries (transborder data flows), especially personal information such as personnel records. Others severely restrict, tax, or prohibit imports of hardware and software. Still others have local content laws that specify the portion of the value of a product that must be added in that country if it is to be sold there. Some countries have reciprocal trade agreements that require a business to spend part of the revenue it earns in a country in that nation's economy.

Geoeconomic challenges in global business and IT refer to the effects of geography on the economic realities of international business activities. The sheer physical distances involved are still a major problem, even in this day of Internet telecommunications and jet travel. For example, it may still take too long to fly in specialists when IT problems occur in a remote site. It is still difficult to communicate in real time across the world's 24 time zones. It is still difficult to get good-quality telephone and telecommunications service in many countries. There are still problems finding the job skills required in some countries or enticing specialists from other countries to live and work there. Finally, there are still problems (and opportunities) in the great differences in the cost of living and labor costs in various countries. All of these geoeconomic challenges must be addressed when developing a company's global business and IT strategies.

Cultural challenges facing global business and IT managers include differences in languages, cultural interests, religions, customs, social attitudes, and political philosophies. Obviously, global IT managers must be trained and sensitized to such cultural differences before they are sent abroad or brought into a corporation's home country. Other cultural challenges include differences in work styles and business relationships. For example, should you take your time to avoid mistakes or hurry to get something done early? Should you go it alone or work cooperatively? Should the most experienced person lead, or should leadership be shared? The answers to such questions depend on the culture you are in and highlight the cultural differences that might exist in the global workplace. Let's take a look at a real-world example about what it takes to be global.

Global CIOs: What Does It Take to Become One?

Let's take the glamorous title of "Global CIO" and break it down into some of the job realities. What do multinational CIOs have to do that their domestic counterparts don't?

First, overcome language and cultural barriers. Then rethink "normal" business practices while coping with IT skill shortages and inexperienced labor pools. Next, build something from nothing. Now connect it to the global corporate infrastructure. Finally, leap tall buildings in a single bound.

That last one might just be the easiest task on the to-do list for IT executives in emerging global markets. "It requires some creativity and new thinking," says Cadbury CIO Wayne Shurts, in a vastly modest understatement of the challenges he and his international colleagues face.

At the same time, fresh approaches from less-developed corners of the world can become testing grounds for new technologies that scale back up to the corporate parent. The emerging markets teams at Cadbury, for example, came up with a sales-force automation tool for smartphones that could end up as part of the candymaker's global applications set. As CIO Shurts notes, the innovative IT mind-set springing up in these green-field markets can be a valuable upgrade for the company's entire global organization.

Because there are more programmers being trained every day in developing parts of the world, IT professionals in the United States are now competing in the global

talent pool, as well. Although many U.S. companies today are still hiring globally only when their need is short-lived, or when skills are scarce or too high-priced in the local or domestic labor pool, some are going global just to find the best of the best, no matter where they're located.

And as many executive recruiters will tell you, CIOs who "go global" somewhere along their career paths develop business muscles their domestic colleagues can't match. The sheer variety of experiences in dealing with developing markets ultimately forges an IT chief who thinks very differently about the world of business.

Will a global tour of duty become a necessity for CIO success in the future?

Source: Adapted from Maryfran Johnson, "The Global CIO Job Description," *CIO*, November 12, 2009; and Mary Brandel, "Swimming in the Global Talent Pool," *Computerworld*, January 15, 2007.

Global Business/IT Strategies

Businesses are moving away from *international* strategies in which foreign subsidiaries are autonomous but depend on headquarters for new processes, products, and ideas; or from *global* strategies, in which a company's worldwide operations are closely managed by corporate headquarters. Instead, companies are moving toward a **transnational strategy**, where the company's business depends heavily on its information systems and Internet technologies to help it integrate its global business activities. Instead of having independent IS units at its subsidiaries, or even a centralized IS operation directed from its headquarters, a transnational business tries to develop an integrated and cooperative worldwide hardware, software, and Internet-based architecture for its IT platform. Figure 14.13 compares the three approaches to global business/IT strategy. Figure 14.14 illustrates how transnational business and IT strategies have been implemented by global companies.

FIGURE 14.13 Companies operating internationally are moving toward transnational business and IT strategies. Note some of the chief differences among international, global, and transnational business and IT strategies.

Comparing Global Business/IT Strategies		
International	**Global**	**Transnational**
• Autonomous operations • Region specific • Vertical integration • Specific customers • Captive manufacturing • Customer segmentation and dedication by region and plant	• Global sourcing • Multiregional • Horizontal integration • Some transparency of customers and production • Some cross regionalization	• Virtual business operations via global alliances • World markets and mass customization • Global e-commerce and customer service • Transparent manufacturing • Global supply chain and logistics • Dynamic resource management
Information Technology Characteristics		
• Stand-alone systems • Decentralized/no standards • Heavy reliance on interfaces • Multiple systems, high redundancy, and duplication of services and operations • Lack of common systems and data	• Regional decentralization • Interface dependent • Some consolidation of applications and use of common systems • Reduced duplication of operations • Some worldwide IT standards	• Logically consolidated, physically distributed, Internet connected • Common global data resources • Integrated global enterprise systems • Internet, intranet, extranet, and Web-based applications • Transnational IT policies and standards

FIGURE 14.14 Examples of how transnational business and IT strategies were implemented by global companies.

Tactic	Global Alliances	Global Sourcing and Logistics	Global Customer Service
Examples	British Airways/US Airways KLM/Northwest Qantas/ American	Benetton	American Express
IT Environment	Global network (online reservation system).	Global network, EPOS terminals in 4,000 stores, CAD/CAM in central manufacturing, robots and laser scanner in automated warehouse.	Global network linked from local branches and local merchants to the customer database and medical or legal referrals database.
Results	• Coordination of schedules • Code sharing • Coordination of flights • Co-ownership	• Produce 2,000 sweaters per hour using CAD/CAM • Quick response (in stores in 10 days) • Reduced inventories (just-in-time)	• Worldwide access to funds • "Global Assist" hotline • Emergency credit card replacement • 24-hour customer service

Global Business/IT Applications

The applications of information technology developed by global companies depend on their **global business/IT strategies** and their expertise and experience in IT. Their IT applications, however, also depend on a variety of **global business drivers**, that is, business requirements caused by the nature of the industry and its competitive or environmental forces. One example would be companies like airlines or hotel chains that have global customers who travel widely or have global operations. Such companies need global IT capabilities for online transaction processing so that they can provide fast, convenient service to their customers—or face losing them to their competitors. The economies of scale provided by global business operations are other business drivers that require the support of global IT applications. Figure 14.15 summarizes some of the business requirements that make global IT a competitive necessity.

Of course, many global IT applications, particularly finance, accounting, and office applications, have been in operation for many years. For example, most multinational

FIGURE 14.15 Some of the business reasons driving global business applications.

Business Drivers of Global IT
• **Global Customers.** Customers are people who may travel anywhere or companies with global operations. Global IT can help provide fast, convenient service.
• **Global Products.** Products are the same throughout the world or are assembled by subsidiaries throughout the world. Global IT can help manage worldwide marketing and quality control.
• **Global Operations.** Parts of a production or assembly process are assigned to subsidiaries based on changing economic or other conditions. Only global IT can support such geographic flexibility.
• **Global Resources.** The use and cost of common equipment, facilities, and people are shared by subsidiaries of a global company. Global IT can keep track of such shared resources.
• **Global Collaboration.** The knowledge and expertise of colleagues in a global company can be quickly accessed, shared, and organized to support individual or group efforts. Only global IT can support such enterprise collaboration.

companies have global financial budgeting, cash management systems, and office automation applications such as fax and e-mail systems. As global operations expand and global competition heats up, however, there is increasing pressure for companies to install global e-commerce and e-business applications for their customers and suppliers. Examples include global e-commerce Web sites and customer service systems for customers, and global supply chain management systems for suppliers. In the past, such systems relied almost exclusively on privately constructed or government-owned telecommunications networks; now the explosive business use of the Internet, intranets, and extranets for e-commerce has made such applications much more feasible for global companies.

Omnicom Group Drives Global ERP Deployment

LUTHRIA/SHUTTERSTOCK

Omnicom Group Inc. is a strategic holding company that manages a portfolio of leading advertising and marketing services agencies. Omnicom has more than 60,000 employees worldwide and reported annual revenue of $13 billion in 2008.

Many of Omnicom's agencies needed more capable and efficient enterprise resource planning (ERP) and accounting systems to meet the increasing client demands for more detailed information and the financial reporting deadlines that the parent company sets.

Zimmerman Advertising, an Omnicom subsidiary that AdWeek ranks as the 14th-largest advertising firm in the United States, was saddled with a cumbersome financial management application. "Our system had not been updated or enhanced in many years—it was in maintenance mode," says Joe Weiner, vice president and corporate controller at Zimmerman. "We were left with few options in terms of improving the existing system. As a result, our financial reporting capabilities were limited and we had minimal ability to reengineer processes and to import and export data."

To improve financial management at its agencies and corporate reporting, Omnicom made the strategic decision to standardize on Microsoft Dynamics AX. "We needed to implement best-in-class financial management software that would allow our agencies to report in faster time frames and meet the varying client demands for information," says Wayne Wilson, global program manager for Omnicom. "Additionally, Microsoft Dynamics AX had the scalability and localization capabilities—both language and statutory—that we required as a global organization."

Omnicom created a template for Microsoft Dynamics AX that would streamline deployments across locations, set standards needed for reporting, and make it easier to customize the solution at the local level to meet the unique needs of individual agencies. For quick and easy access to information, Omnicom implemented Enterprise Portal for Microsoft Dynamics AX, which provides Web-based access to key information.

At Zimmerman, the efficiencies gained with the new system have been dramatic. "Microsoft Dynamics AX offers a multidimensional chart of accounts that vastly improves our revenue and expense reporting," says Chuck Miller, financial systems manager at Zimmerman. "We're also seeing many other efficiencies in our processes.

We save 80 hours each month with our new process for importing transactions, and our ability to capture more detailed information is better as well. We're also using the online document-handling function to save and retrieve documents electronically, and we have established automatic workflows."

"As a global company, we had to ensure we had alignment between our strategic goals at the corporate level and the individual implementations that were occurring throughout the agencies," explains Wilson. "We aligned the Microsoft product, our corporate goals, and the agencies' local requirements. The coordinated efforts of the consulting and development teams made it so that knowledge gained in one area of the program was incorporated into other areas of the program."

Source: Adapted from *Microsoft Case Study*, "Omnicom Group Drives Global ERP Deployment with Strategy and Development Support," January 29, 2010.

Global IT Platforms

The management of technology platforms (also called the technology infrastructure) is another major dimension of global IT management—that is, managing the hardware, software, data resources, telecommunications networks, and computing facilities that support global business operations. The management of a global IT platform not only is technically complex but also has major political and cultural implications.

For example, hardware choices are difficult in some countries because of high prices, high tariffs, import restrictions, long lead times for government approvals, lack of local service or spare parts, and lack of documentation tailored to local conditions. Software choices can also present unique problems. Software packages developed in Europe may be incompatible with American or Asian versions, even when purchased from the same hardware vendor. Well-known U.S. software packages may be unavailable because there is no local distributor or because the software publisher refuses to supply markets that disregard software licensing and copyright agreements.

Managing international data communications networks, including Internet, intranet, extranet, and other networks, is a key global IT challenge. Figure 14.16 outlines the top 10 international data communications issues as reported by IS executives at 300 Fortune 500 multinational companies. Notice how political issues dominate the top 10 listing over technology issues, clearly emphasizing their importance in the management of global telecommunications.

Establishing computing facilities internationally is another global challenge. Companies with global business operations usually establish or contract with systems integrators for additional data centers in their subsidiaries in other countries. These data centers meet local and regional computing needs and even help balance global computing workloads through communications satellite links. Offshore data centers, however, can pose major problems in headquarters' support, hardware and software acquisition, maintenance, and security. That's why many global companies turn to application service providers or systems integrators like EDS or IBM to manage their overseas operations.

FIGURE 14.16
The top 10 issues in managing international data communications.

International Data Communications Issues
Network Management Issues
• Improving the operational efficiency of networks
• Dealing with different networks
• Controlling data communication security
Regulatory Issues
• Dealing with transborder data flow restrictions
• Managing international telecommunication regulations
• Handling international politics
Technology Issues
• Managing network infrastructure across countries
• Managing international integration of technologies
Country-Oriented Issues
• Reconciling national differences
• Dealing with international tariff structures

Source: Adapted from Vincent S. Lai and Wingyan Chung, "Managing International Data Communications," *Communications of the ACM,* March 2002, p. 91.

Orbitz.com: Toward an Integrated Global Platform

Originally established through a partnership of major airlines, and subsequently owned by various entities, Orbitz.com—the flagship brand of Orbitz Worldwide—has been in operation since 2001. Now it's undertaking a major upgrade to improve its online platform and enhance its ability to do business worldwide. All of this has to happen without disrupting Orbitz's ongoing operations.

Orbitz must interface with an array of systems to conduct business: It still has ties into the reservation systems of its original airline owners and those of other airlines it has partnered with along the way. It also must tap into the global distribution systems that still account for a great deal of the airline reservation business. And Orbitz isn't only about airline tickets. The real action and the real profits in the travel industry these days are in hotel rooms, car rentals, train trips, luxury cruises, bus tours, event tickets, and all of that rolled up into vacation packages.

Orbitz was left without a CIO after the departure of Bahman Koohestani. "I certainly understand enough about IT to run this organization," says Mike Nelson, chief operations officer, who has a background in financial planning and operations, not technology.

Jack Staehler, group vice president of technology, isn't worried about the lack of a CIO title. "The global platform, that's my charter," he says.

Code-named Austin, Orbitz's new online platform is a component-based system that uses a great deal of the Java code underpinning Orbitz's current platform.

What's different is that it can support multiple Web sites, both internal and external to Orbitz. It features standards-based user-interface technology able to incorporate dynamic updates and accessible from a range of devices. The idea is to be able to plug in data feeds from Orbitz's systems, like CheapTickets.com, and those of its partners and potential partners. It's multilingual and multicurrency, yet location specific.

For example, it understands what a domestic flight is wherever it's being accessed; previously, "domestic" was hardwired into the Orbitz system as referring to the United States.

Orbitz began rolling out Austin in 2008, starting with the Ebookers site in England. "The new Web site aims to make booking decisions easier through simpler navigation and more product choice," the company said in a release. Hooking into the Orbitz system, for instance, tripled hotel inventory available to Ebookers customers.

One reason Orbitz is in such a hurry is that the online travel industry isn't standing still. Travel search engines like Kayak.com, which can operate across platforms, threaten online travel sites with some of the same disintermediation that travel sites brought to travel agencies years ago. And some observers wonder when, not if, the 800-pound Internet gorilla, Google, will enter the online travel market.

"We're trying to accelerate this as much as possible, but it's a huge task," Nelson says. "You can only throw bodies at it so much, and that doesn't mean it's going to happen any faster."

Source: Adapted from John Soat, "Orbitz's Long, Strange Trip to a New Online Platform," *InformationWeek*, February 9, 2008.

The Internet as a Global IT Platform

What makes the Internet and the World Wide Web so important for international business? This interconnected matrix of computers, information, and networks that reaches tens of millions of users in over one hundred countries is a business environment free of traditional boundaries and limits. Linking to an online global infrastructure offers companies unprecedented potential for expanding markets, reducing costs, and improving profit margins at a price that is typically a small percentage of the corporate communications budget. The Internet provides an interactive channel for direct communication and data exchange with customers, suppliers, distributors, manufacturers, product developers, financial backers, information providers—in fact, with all parties involved in a given business venture.

So the Internet and the World Wide Web have now become vital components in international business and commerce. Within a few years, the Internet, with its

FIGURE 14.17
Key questions for companies establishing global Internet Web sites.

Key Questions
• Will you have to develop a new navigational logic to accommodate cultural preferences?
• What content will you translate, and what content will you create from scratch to address regional competitors or products that differ from those in the United States?
• Should your multilingual effort be an adjunct to your main site, or will you make it a separate site, perhaps with a country-specific domain name?
• What kinds of traditional and new media advertising will you have to do in each country to draw traffic to your site?
• Will your site get so many hits that you'll need to set up a server in a local country?
• What are the legal ramifications of having your Web site targeted at a particular country, such as laws on competitive behavior, treatment of children, or privacy?

interconnected network of thousands of networks of computers and databases, has established itself as a technology platform free of many traditional international boundaries and limits. By connecting their businesses to this online global infrastructure, companies can expand their markets, reduce communications and distribution costs, and improve their profit margins without massive cost outlays for new telecommunications facilities. Figure 14.17 outlines key considerations for global e-commerce Web sites.

The Internet, along with its related intranet and extranet technologies, provides a low-cost interactive channel for communications and data exchange with employees, customers, suppliers, distributors, manufacturers, product developers, financial backers, information providers, and so on. In fact, all parties involved can use the Internet and other related networks to communicate and collaborate to bring a business venture to its successful completion. As Figure 14.18 illustrates, amazing growth has occurred worldwide with regard to the Internet; however, much work needs to be done to bring secure Internet access and e-commerce to more people in more countries. Nonetheless, the trend is clearly toward continued expansion of the Internet as it becomes a pervasive IT platform for global business.

Global Data Access Issues

Global **data access issues** have been a subject of political controversy and technology barriers in global business operations for many years but have become more visible with the growth of the Internet and the pressures of e-commerce. A major example is the issue of

FIGURE 14.18 Current numbers of Internet users by world region. Note: Internet usage and population statistics, updated on December 31, 2009.

World Internet Usage and Population Statistics						
World Regions	Population (2009 Est.)	Population (% of World)	Internet Usage, Latest Data	Usage Growth 2000–2009 (%)	Penetration (% Population)	World Users (%)
Africa	991,002,342	14.0	86,217,900	1,809.8	8.7	4.8
Asia	3,808,070,503	56.3	764,435,900	568.8	20.1	42.4
Europe	803,850,808	11.4	425,773,571	305.1	53.0	23.6
Middle East	202,687,005	4.0	58,309,546	1,675.1	28.8	3.2
North America	340,831,831	5.1	259,561,000	140.1	76.2	14.4
Latin America/Caribbean	586,662,468	8.5	186,922,050	934.5	31.9	10.4
Oceania/Australia	34,700,201	0.5	186,922,050	177.0	60.8	1.2
WORLD TOTAL	**6,767,805,208**	**100.0**	**1,802,330,457**	**399.3**	**26.6**	**100.0**

Source: www.internetworldstats.com.

FIGURE 14.19
Key data privacy provisions of the agreement to protect the privacy of consumers in e-commerce transactions between the United States and the European Union.

U.S.–E.U. Data Privacy Requirements
• Notice of purpose and use of data collected
• Ability to opt out of third-party distribution of data
• Access for consumers to their information
• Adequate security, data integrity, and enforcement provisions

transborder data flows (TDF), in which business data flow across international borders over the telecommunications networks of global information systems. Many countries view TDF as a violation of their national sovereignty because these data flows avoid customs duties and regulations for the import or export of goods and services. Others view TDF as a violation of their laws to protect the local IT industry from competition or their labor regulations for protecting local jobs. In many cases, the data flow business issues that seem especially politically sensitive are those that affect the movement out of a country of personal data in e-commerce and human resource applications.

Many countries, especially those in the European Union (E.U.), may view transborder data flows as a violation of their privacy legislation because, in many cases, data about individuals are being moved out of the country without stringent privacy safeguards. For example, Figure 14.19 outlines the key provisions of a data privacy agreement between the United States and the European Union. The agreement exempts U.S. companies engaging in international e-commerce from E.U. data privacy sanctions if they join a self-regulatory program that provides E.U. consumers with basic information about, and control over, how their personal data are used. Thus, the agreement is said to provide a "safe harbor" for such companies from the requirements of the E.U.'s Data Privacy Directive, which bans the transfer of personal information on E.U. citizens to countries that do not have adequate data privacy protection.

Europe: Tighter Laws Worry Security Professionals

Moves by several European countries to tighten laws against computer hacking worry security professionals who often use the same tools as hackers but for legitimate purposes. The United Kingdom and Germany are among the countries that are considering revisions to their computer crime laws in line with the 2001 Convention on Cybercrime, a Europe-wide treaty, and with a similar E.U. measure passed in early 2005.

But security professionals are scrutinizing those revisions out of concern for how prosecutors and judges could apply the laws. Security professionals are especially concerned about cases where the revisions apply to programs that could be used for bad or good. Companies often use hacking programs to test the mettle of their own systems.

"One useful utility in the wrong hands is a potentially malicious hacking tool," says Graham Cluley, senior technology consultant at Sophos in Abingdon, England. The proposed revisions would make it illegal to create or supply a tool to someone who intends to use it for unauthorized computer access or modification. Likewise, the proposed changes to German law would also criminalize making and distributing hacking tools. The German government said the changes will bring it into compliance with the 2001 Convention on Cybercrime. Several German security companies are planning to lobby against the law, as they fear it could hamper those who test security systems, says Alexander Kornbrust, founder and chief executive officer of Red-Database-Security in Neunkirchen, Germany. For example, tools to check the strength of passwords, often freely distributed, could also be used by malicious hackers, he says.

"The security community is very unhappy with this approach," Kornbrust says. "The concern is that the usage and possession of so-called hacker tools will become illegal."

The United Kingdom and Germany are trying to align their laws with Article 6 of the convention, which bans the creation of computer programs for the purpose of committing cyber-crime. So far, 43 countries have signed the convention, which indicates their willingness to revise their laws to comply. Fifteen have ratified the convention. After a country changes its laws, it can ratify the convention and put it into force.

Source: Adapted from Dave Gradijan, "Euro Computer Crime Laws Have Security Pros Worried," *CSO Magazine*, September 29, 2006.

Internet Access Issues

The Paris-based organization Reporters Without Borders (RSF) reports that there are 45 countries that "restrict their citizens' access to the Internet." At its most fundamental, the struggle between Internet censorship and openness at the national level revolves around three main means: controlling the conduits, filtering the flows, and punishing the purveyors. In countries such as Burma, Libya, North Korea, Syria, and the countries of Central Asia and the Caucasus, Internet access is either banned or subject to tight limitations through government-controlled ISPs, says the RSF.

Figure 14.20 outlines the restrictions to public **Internet access** by the governments of the countries deemed most restrictive by the Paris-based Reporters Without Borders (RSF). See their Web site at www.rsf.fr.

As an example, Internet censorship in the People's Republic of China is conducted under a wide variety of laws and administrative regulations. In accordance with these laws, more than sixty Internet regulations have been made by the People's Republic of China (PRC) government, and censorship systems are vigorously implemented by provincial branches of state-owned ISPs, business companies, and organizations. Most national laws of the People's Republic of China do not apply to the Special Administrative Regions of Hong Kong or Macau. There are no known cases of the PRC authorities censoring critical political or religious content in those areas.

The escalation of the government's effort to neutralize critical online opinion comes after a series of large anti-Japanese, anti-pollution and anti-corruption protests, many of which were organized or publicized using instant messaging services, chat rooms, and text messages. The size of the Internet police is estimated at more than 30,000. Critical comments appearing on Internet forums, blogs, and major portals such as Sohu and Sina usually are erased within minutes.

The apparatus of the PRC's Internet repression is considered more extensive and more advanced than in any other country in the world. The regime not only blocks Web site content but also monitors the internet access of individuals. Amnesty International notes that China "has the largest recorded number of imprisoned journalists and cyber-dissidents in the world." The offenses of which they are accused include communicating with groups abroad, opposing the persecution of the Falun Gong, signing online petitions, and calling for reform and an end to corruption.

FIGURE 14.20
Countries that restrict or forbid Internet access by their citizens.

Global Government Restrictions on Internet Access
● **High Government Access Fees** Kazakhstan, Kyrgyzstan
● **Government-Monitored Access** China, Iran, Saudi Arabia, Azerbaijan, Uzbekistan
● **Government-Filtered Access** Belarus, Cuba, Iraq, Tunisia, Sierra Leone, Tajikistan, Turkmenistan, Vietnam
● **No Public Access Allowed** Burma, Libya, North Korea

So the Internet has become a global battleground over public access to data and information at business and private sites on the World Wide Web. Of course, this becomes a business issue because restrictive access policies severely inhibit the growth of e-commerce with such countries. Most of the rest of the world has decided that restricting Internet access is not a viable policy but in fact would hurt their countries' opportunities for economic growth and prosperity. Instead, national and international efforts are being made to rate and filter Internet content deemed inappropriate or criminal, such as Web sites for child pornography or terrorism. In any event, countries that significantly restrict Internet access are also choosing to restrict their participation in the growth of e-commerce.

To RSF and others, these countries' rulers face a losing battle against the Information Age. By denying or limiting Internet access, they stymie a major engine of economic growth. By easing access, however, they expose their citizenry to ideas that potentially might destabilize to the status quo. Either way, many people will get access to the electronic information they want. "In Syria, for example, people go to Lebanon for the weekend to retrieve their e-mail," says Virginie Locussol, RSF's desk officer for the Middle East and North Africa.

Global Systems Development

Just imagine the challenges of developing efficient, effective, and responsive applications for business end users domestically. Then, multiply that by the number of countries and cultures that may use a global e-business system. That's the challenge of managing global systems development. Naturally, there are conflicts over local versus global system requirements, as well as difficulties agreeing on common system features, such as multilingual user interfaces and flexible design standards. All of this effort must take place in an environment that promotes involvement and "ownership" of a system by local end users.

Other **systems development issues** arise from disturbances caused by systems implementation and maintenance activities. For example, "An interruption during a third shift in New York City will present midday service interruptions in Tokyo." Another major development issue relates to the trade-offs between developing one system that can run on multiple computer and operating system platforms or letting each local site customize the software for its own platform.

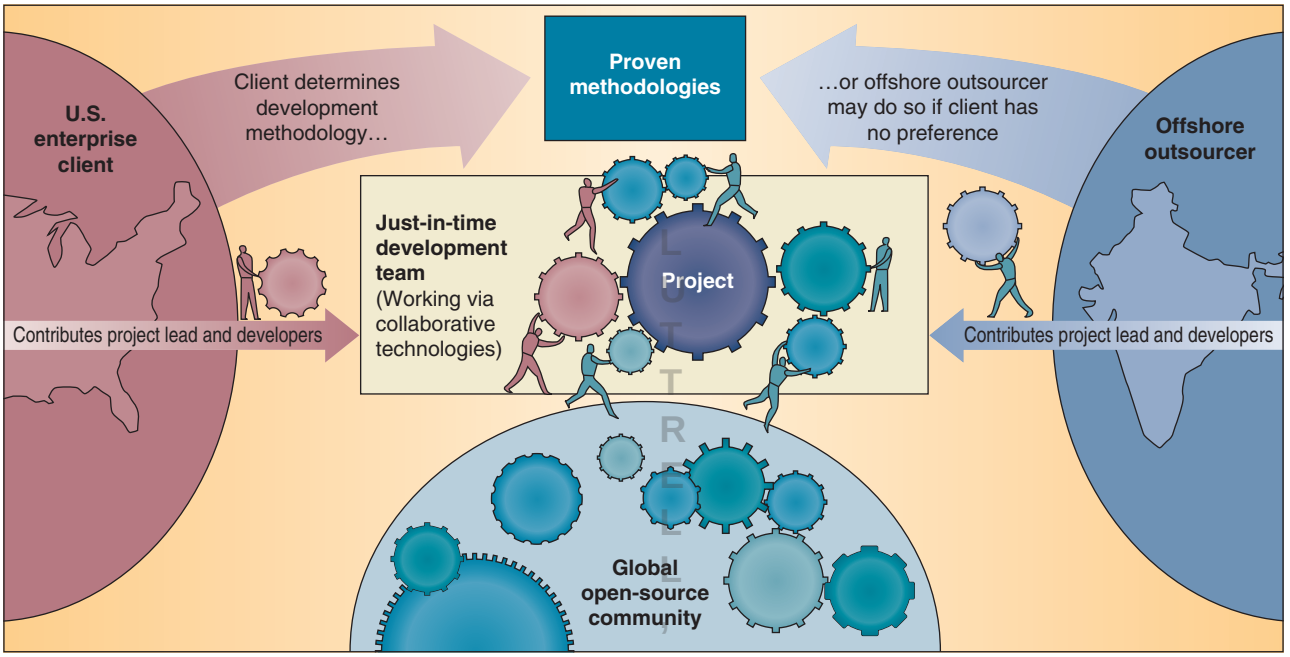
Other important global systems development issues are concerned with global standardization of data definitions. Common data definitions are necessary for sharing data among the parts of an international business. Differences in language, culture, and technology platforms can make global data standardization quite difficult. For example, a sale may be called an "order booked" in the United Kingdom, an "order scheduled" in Germany, and an "order produced" in France. Yet, businesses are moving ahead to standardize data definitions and structures. By moving their subsidiaries into data modeling and database design, they hope to develop a global data architecture that supports their global business objectives.

Systems Development Strategies

Several strategies can be used to solve some of the systems development problems that arise in global IT. The first strategy is to transform an application used in the home office into a global application. Often, the system that has the best version of an application will be chosen for global use. Another approach is to set up a *multinational development team* with key people from several subsidiaries to ensure that the system design meets the needs of local sites, as well as corporate headquarters.

A third approach is called *parallel development*. That's because parts of the system are assigned to different subsidiaries and the home office to develop at the same time, based on the expertise and experience at each site. Another approach is the concept of *centers of excellence*. In this approach, an entire system may be assigned for development to a particular subsidiary based on its expertise in the business or technical dimensions needed for successful development. A final approach that has rapidly become a major

FIGURE 14.21 An example of Internet-enabled collaboration in global IT systems development. Note the roles played by the client company, off-shore outsource developer, global open-source community, and just-in-time development team.



Source: Adapted from Jon Udell, "Leveraging a Global Advantage," *Infoworld*, April 21, 2003, p. 35.

development option is to outsource the development work to global or *offshore* development companies that have the skills and experience required to develop global business/IT applications. Obviously, all of these approaches require development team collaboration and managerial oversight to meet the global needs of a business. So, global systems development teams are making heavy use of the Internet, intranets, groupware, and other electronic collaboration technologies. See Figure 14.21.

Invensys PLC: Drawing Talent from Around the World for Software Development

It's great being able to draw upon your best programmers from throughout the world. SimSci-Esscor, the industrial process simulation and control unit of Invensys PLC, will assign personnel from any of its offices to assemble the right team. "Our development projects operate in a virtual mode and gather people from multiple sites based on project needs," says Joe Ayers, director of development services at SimSci-Esscor in Lake Forest, California. "It is common for projects to utilize developers from three different time zones in a 'follow the sun' development mode."

The approach allows Invensys to find the right talent for the project, and work is done in an efficient way. But managing those far-flung developers can be a nightmare. "Invensys had brought together multiple companies with different cultures and processes," Ayers explains. "Some of the issues we have had to address include duplication of source code, multiple tools and processes in use, and limited network connectivity and reliability."

To tackle these issues, Invensys created a virtual development infrastructure for 135 developers in five locations. To facilitate communication, it incorporated desktop-sharing tools, instant messaging, conference calling, and voice-over-IP technology.

For working on the code itself, the company deployed three products from Telelogic AB in Malmo, Sweden: Synergy/CM for controlling project configuration items, Synergy/Change for controlling change requests, and Synergy/Distributed CM for synchronizing change requests and source code between databases at multiple

sites. It also implemented a wide-area file-sharing system from Availl Inc. in Andover, Massachusetts, for other documents. "With this development structure, we have the ability to add or remove changes to software builds at the last minute, with no project-delivery slips attributed to distributed development complexity over the last year," says Ayers. "We've been able to lower project start-up time and project costs."

Experts say managing distributed development teams requires a mix of processes and tools. "Rarely is it a problem with the technology, though that used to be a major hurdle in the past," says Dale Karolak, vice president of product development at Intier Automotive Inc. in Novi, Michigan, and author of *Global Software Development: Managing Virtual Teams and Environments*. "Most problems now are with communications, documentation and alignment." Karolak says managers need to exert more discipline when it comes to scheduling and holding meetings and tracking project targets, and spend more time visiting off-site locations for face-to-face meetings. Proper management also requires a greater awareness of potential problems.

"Jump on problems right away. Don't wait," Karolak says. "Longer distances will cause longer delays in solving the issues if they are not addressed quickly."

Source: Adapted from Drew Robb, "Global Workgroups," *Computerworld*, August 15, 2005.

Summary

- **Managing Information Technology.** This can be viewed as managing three major components: (1) the joint development and implementation of e-business and IT strategies, (2) the development of e-business applications and the research and implementation of new information technologies, and (3) IT processes, professionals, and subunits within a company's IT organization and IS function.
- **Failures in IT Management.** Information systems are not being used effectively or efficiently by many organizations. The experiences of successful organizations reveal that the basic ingredient of high-quality information system performance is extensive and meaningful management, as well as user involvement in the governance and development of IT applications. Thus, managers may serve on executive IT groups and create IS management functions within their business units.
- **Managing Global IT.** The international dimensions of managing global information technologies include dealing with cultural, political, and geoeconomic challenges posed by various countries; developing appropriate business and IT strategies for the global marketplace; and developing a portfolio of global e-business and e-commerce applications and an Internet-based technology platform to support them. In addition, data access methods have to be developed and systems development projects managed to produce the global e-business applications that are required to compete successfully in the global marketplace.
- **Global Business and IT Strategies and Issues.** Many businesses are becoming global companies and moving toward transnational business strategies in which they integrate the global business activities of their subsidiaries and headquarters. This transition requires that they develop a global IT platform—that is, an integrated worldwide hardware, software, and Internet-based network architecture. Global companies are increasingly using the Internet and related technologies as a major component of this IT platform to develop and deliver global IT applications that meet their unique global business requirements. Global IT and end-user managers must deal with limitations to the availability of hardware and software; restrictions on transborder data flows, Internet access, and movement of personal data; and difficulties with developing common data definitions and system requirements.

Key Terms and Concepts

These are the key terms and concepts of this chapter. The page number of their first explanation is in parentheses.

1. Application development management (586)
2. Business/IT planning process (583)
3. Centralization or decentralization of IT (586)
4. Chargeback systems (587)
5. Chief information officer (CIO) (588)
6. Chief technology officer (CTO) (589)

7. Data center (587)
8. Downsizing (586)
9. Global business drivers (604)
10. Global information technology management (598)
    a. Data access issues (608)
    b. Systems development issues (611)
11. IS operations management (587)
12. IT architecture (584)
13. IT staff planning (588)
14. Management and end-user involvement (594)
15. Managing information technology (580)
16. Offshoring (591)
17. Outsourcing (590)
18. System performance monitor (587)
19. Technology management (589)
20. Transborder data flows (TDF) (609)
21. Transnational strategy (603)
22. User services (589)

Review Quiz

Match one of the key terms and concepts listed previously with one of the brief examples or definitions that follow. Try to find the best answer, even though some seem to fit more than one term or concept. Defend your choices.

____ 1. Focuses on discovering innovative approaches to satisfying a company's customer value and business value goals with the support of IT.

____ 2. Concerned with the use of hardware, software, network, and IS personnel resources within the corporate or business unit.

____ 3. Managing business/IT planning and the IS function within a company.

____ 4. A conceptual design, or blueprint, of an organization's IS/IT functions, hardware, and software created by a strategic business/IT planning process.

____ 5. Many organizations have both centralized and decentralized IT units.

____ 6. Managing the creation and implementation of new business applications.

____ 7. End users need liaison, consulting, and training services.

____ 8. Involves recruiting, training, and retaining qualified IS personnel.

____ 9. Corporate locations for computer system operations.

____ 10. Rapidly changing technological developments must be anticipated, identified, and implemented.

____ 11. A relocation of an organization's business processes (including production/manufacturing) to a lower-cost location, usually overseas.

____ 12. The executive responsible for strategic business/IT planning and IT management.

____ 13. The executive in charge of researching and implementing new information technologies.

____ 14. Software that helps monitor and control computer systems in a data center.

____ 15. The cost of IS services may be allocated back to end users.

____ 16. Many business firms are replacing their mainframe systems with networked PCs and servers.

____ 17. The purchase of goods or services from third-party partners that were previously provided internally.

____ 18. Managing IT to support a company's international business operations.

____ 19. A business depends heavily on its information systems and Internet technologies to help it integrate its global business activities.

____ 20. Global customers, products, operations, resources, and collaboration.

____ 21. Global telecommunications networks like the Internet move data across national boundaries.

____ 22. Agreement is needed on common user interfaces and Web site design features in global IT.

____ 23. Security requirements for personal information in corporate databases within a host country are a top concern.

____ 24. Business managers should oversee IT decision making and projects that are critical to their business units' success.

Discussion Questions

1. What has been the impact of information technologies on the work relationships, activities, and resources of managers?
2. What can business unit managers do about performance problems in the use of information technology and the development and operation of information systems in their business units?
3. Refer to the Real World Case on BP's IT transformation in the chapter. Dana Deasy discusses the long-term benefits of "embedded IT" while noting the need to

centralize the department in the short term. How does one organization make the transition from one approach to the other? What does it take to be successful in this regard?

4. How are Internet technologies affecting the structure and work roles of modern organizations? For example, will middle management wither away? Will companies consist primarily of self-directed project teams of knowledge workers? Explain your answers.
5. Should the IS function in a business be centralized or decentralized? Use the Internet to find recent developments to support your answer.
6. Refer to the Real World Case on the globalization challenges faced by CIOs in the chapter. All those mentioned are CIOs from headquarters who went abroad, but there is no mention of CIOs from emerging countries taking over the global helm. Why do you think this is the case?
7. How might cultural, political, or geoeconomic challenges affect a global company's use of the Internet? Give several examples.
8. Will the increasing use of the Internet by firms with global business operations change their move toward a transnational business strategy? Explain.
9. How might the Internet, intranets, and extranets affect the business drivers or requirements responsible for a company's use of global IT, as shown in Figure 14.13? Give several examples to illustrate your answer.

Analysis Exercises

1. Top-Rated Web Sites for Executives

CEO Express

Check out CEO Express (www.ceoexpress.com), a top-rated Web portal for busy executives. See Figure 14.22. The site provides links to top U.S. and international newspapers, business and technology magazines, and news services. Hundreds of links to business and technology research sources and references are provided, as well as travel services, online shopping, and recreational Web sites. Premium services include e-mail, contact management, calendaring and scheduling, community networking, and powerful information organizing and sharing tools.

a. Evaluate the CEO Express Web site as a source of useful links to business and technology news, analysis, and research sources for business executives and professionals.

b. Compare CEO Express with Google News (news.google.com) and Google IG (www.google.com/ig). What advantages does CEO Express provide?

c. Select the featured article from the "Editor's Corner." What was the source? Summarize the article. Was it useful to you?

FIGURE 14.22
The CEO Express Web site.

Source: Courtesy of CEO Express.

2. **Information and Communications for Development**
Assessing Global Capabilities
More than one billion people take their electrical and telecommunications systems for granted. However, for billions more, the service-on-demand mentality remains a distant dream and Internet access only a rumor. Recognizing the need to promote global information and communications technologies (GICT), the World Bank has undertaken numerous technology infrastructure assessment and development projects.
   a. What is the World Bank (www.worldbank.org) doing to address third-world computer literacy needs?
   b. What is MIT (www.mit.edu) doing to help increase global computer literacy?

3. **Overseas Assignments**
Incompatible Electricity?
Business travelers who need to remain connected face special challenges outside their home country, especially those who work out of their hotel rooms. Electricity varies by voltage, cycles, and electric-plug shape. Likewise, telephone jacks may vary from country to country and, for the most part, American cell phones work only in America.
   If you find yourself on an overseas assignment, how will you keep your laptop computer charged? How will you access the Internet? Can you free yourself from expensive hotel telephone surcharges?
   Pick a country to "visit" (your professor may assign one instead), and report on specific solutions to each question. Be sure to include the manufacturer and model number of any hardware you may require. Cite all your sources.
   a. What do you need to bring with you to keep your laptop computer charged?
   b. What do you need to bring with you to connect your laptop's modem to the local telephone network?
   c. What will you use in place of your handy cell phone?
   d. Use a collaboration-enabled system such as Blackboard, Web CT, Dreamweaver, or Front Page to merge, organize, and publish your results with the rest of your class to create an online resource.

4. **Knowledge Work on the Move**
Business Process Outsourcing
As a result of the location independence of knowledge work, many organizations seek to lower their labor costs by moving their digital operations overseas. When managers evaluate such opportunities, they must consider the following regional attributes:

- Political and regulatory environment
- Infrastructure (electrical, telecommunications)
- Professionally skilled labor force
- Information systems skilled labor force

All prospective locations must have a supportive political and regulatory environment; however, variations within the other three attributes will pose special limitations. For example, India has millions of well-educated workers but notoriously unreliable telecommunications and electrical grids. Organizations that set up outsourcing operations in India build their own islands of stability with backup power and satellite telecommunications systems. A region with a shortage of professionally skilled labor may offer labor-intensive activities such as call centers or data entry instead, yet even these jobs require basic computer literacy.
   The value of services provided depends primarily on the expertise or creativity involved in its performance. List suitable job titles for each work characteristic below. Rank each item in order of the value provided.
   a. Digitize: Convert data or information into a digital form.
   b. Distribute: Process information in one direction or another based on strict rules and nondigital inputs (if the inputs were digital, a computer could probably do the job).
   c. Analyze: Process information based on human expertise.
   d. Create: Create new information or products based on human expertise.

REAL WORLD CASE 3

Toyota, Procter & Gamble, Hess Corporation, and Others: Retiring CIOs and the Need for Succession Planning

LUTTRELL, SONYA LOUISE 256668U

Barbra Cooper started as a CIO when the position was still called "vice president of information services." In her more than 30 years in IT, she's seen the role become ever more strategic. Until now, the CIO is in the unique position of being the C-level officer who can "see across the entire enterprise."

As the CIO for Toyota Motor Sales USA, Cooper thinks tomorrow's CIOs will be even more strategic and influential, but she also worries about the future business and technology changes they face. "The next 10 to 20 years are going to be challenging," she says. As she talks about the challenges that lie ahead, the question arises: Where will the IT leaders come from to tackle them?

It's a question more and more IT executives are asking themselves. CIOs are moving up and out. The first full-career CIO generation is beginning to retire. Others are increasingly taking on broader responsibilities or moving out of IT and into other business leadership roles as the position evolves beyond its technology roots. In fact, CIO's 2008 State of the CIO report found that 56 percent of CIOs surveyed say long-term strategic thinking and planning is the executive leadership skill most critical in their current role, followed by collaboration and influence (47 percent), and expertise running IT (39 percent). At the same time, many CIOs don't know who would lead IT if they left tomorrow. When you consider that just 17 percent of respondents to the State of the CIO survey cited people development as a critical leadership competency, that's not surprising.

The skills to be CIO have also changed as the role has shifted from technologist to business strategist. It used to be that "we could afford to let the business tell us what they wanted us to do, be good at delivering it and keep our jobs," says Cooper. "Now, the physics and velocity of business and its demands mean you can't afford to wait until something happens."

Indeed, CEOs now look to the CIO to act more as a strategic business leader and less as a function head. TAC Worldwide CEO Robert Badavas says he seldom speaks about technology with his CIO; instead, the two talk about "shaping the business value to our clients," he says. To be successful, he notes, the CIO needs to understand the value proposition of the business. "By staying in the silo of technology, HR, accounting or any other," says Badavas, "you're not going to be as valuable to the business." Or to the CEO.

With all that in mind, CIOs today must groom not only competent replacements for themselves but also next-generation IT leaders who are "business ready" and able to succeed in a more IT-intense and integral business environment. The shift in business expectations means that CIOs have better job security than in the past.

It also takes longer to find good ones with the right mix of business and technical know-how. For example, Pete Walton is in his second stint as CIO at Hess Corp. The petroleum products company coaxed him out of retirement in 2005 when its CIO at that time left. Hess wanted someone who could take its Information Services "to the next level," says Walton.

"CEOs want someone who's business savvy and can figure out how you can use technology for the business. Trying to find that hybrid person is hard," says Diane S. Wallace, chief information officer for the state of Connecticut. It will only get harder to find them, just for demographic reasons. "We have this triple threat of labor shortage: The Boomers are retiring, young people are not going into IT and fewer people are getting degrees," says Robert D. Scott, who in February retired as Procter & Gamble's vice president of global business services. Scott says he noticed a drop in IT interest during the technology bubble of the late 1990s.

Then the rush to outsourcing created a cloud around U.S. IT jobs. That pall persists despite strong job growth in IT, which is expected to add more than 200,000 jobs by 2016, according to the Bureau of Labor Statistics.

Procter & Gamble (P&G) is a case in point. It outsourced about half of its IT staff in 2003, but IT employment is now back to the level it was five years ago. Scott says that this is because the company outsourced its commodity IT, and "internal IT moved up the food chain, and is creating more and more business value."

Scott says P&G continues to attract strong candidates for IT jobs, but the hiring pool is not as deep as in years past. Plus, P&G believes strongly in promoting people steeped in its culture. It worries about keeping its Generation Y employees. The triple threat is already creating an IT brain drain. Wallace says 40 percent of her staff of 518 will be eligible for retirement in the next two to three years. Barbara A. White, chief information officer and associate provost at the University of Georgia, says that when three staff members retired in April, she lost their combined 90 years of experience, and she has a lot of staff likely to retire in the next 10 years.

Toyota's Cooper is dedicating time to prepare her organization for the future, which includes being as proactive as possible and staying ahead of the business needs. It also means a commitment to active succession planning. Two years ago, Cooper sat down for 90 minutes with 27 team members who reported either directly to her or directly to another team member. Each meeting was an open coaching session structured around her ideas of what IT leaders will need to be in 10 years. She then crafted a three- to four-page letter for each team member, detailing the capabilities she wanted them to develop and a plan for showing how they were achieving them. Those who reported directly to her received a summary of what she sent to their team members.

Procter & Gamble has a corporate culture that promotes from within. It saw, however, that good technical talent was getting harder to keep, and it also understood that

Generation Y employees expect to change companies frequently. To combat both challenges, it blazed a new, faster IT career path for its younger workers.

IT leadership adopted an accelerated development program, as a part of the career path, says Scott. It would place a new set of top performers in a Career Executive Development Program, designed to provide them exposure to high-level IT executives and assignments to help accelerate their growth. It comes with one caveat: If you don't perform, you'll be looking for another employer. It's a modified version of what's in place in the company's fabled brand management department.

"We wanted to signal that we were very serious about growing people, and were willing to invest extra time and energy" in them, he says. The program is only two years old and is too new to have clear results (no one, for instance, has been asked to leave yet).

P&G also created what it calls "The CIO Circle," which rewards long-time IT people who have mastered an area of technical expertise. This "master's" designation allows P&G to acknowledge their status as knowledge leaders even if they are not on the management track. Rewards programs encourage employee loyalty, says Laurie Orlov, a consultant and principal of LMO Insight. Fast-track development in particular should help companies cultivate Generation Y leaders. With so much training and management exposure, they have every reason to stay, she says.

Chief information officers who are serious about developing leaders in their group have to be willing to invest time in their people and to give them opportunities to grow, even if that means sometimes letting them fail. It might also mean getting out of their way when the time comes. Hess Corp.'s Walton says that his goal at all of his jobs has been to identify and develop replacements for himself. "You do that by creating opportunities for them, you make them look like leadership heroes in the eyes of their business and let them take all the glory," says Walton, who is 63 and retired from Hess for the second time last month after the company named Jeff Steinhorn, who served under Walton, as its new CIO.

Like most chief information officers who aim to develop their staff, Walton has used a multipronged strategy for helping people along: He mentors, he provides role models, he moves staff into new opportunities, and he invests heavily in education. In fact, he sent selected top managers to a Harvard Business School executive program, and IT has two memberships to the BSG Concours Group, a strategy and executive education firm.

Walton sees the coming leadership challenge as a plus, not a minus. "There is a gap, but it's an exciting one to fill," he says. For one thing, Walton thinks the blend of experience and technical savvy available when you mix Baby Boomers and Generation Y is a powerful one for companies that work to bring these generations together.

He is talking with Hess about how to do it, and he may want to take on such a role in the future. Now that a new IT leader is in place at Hess, however, Walton can relax for a bit. "I'm going to get my [golf] handicap down," he says.

Source: Adapted from Michael Fitzgerald, "How to Develop the Next Generation of IT Leaders," *CIO Magazine*, May 2, 2008.

CASE STUDY QUESTIONS

1. Several comments in the case note that chief information officers are in a unique position for companywide leadership, extending beyond their primary technological concerns. Why do you think this is the case? How are CIOs different in this regard from other chief officers, for example, in finance, HR, or marketing?
2. After reading the case, what do you think are the most important competencies for the successful CIO of tomorrow? How do you rate yourself in those? Have you considered the importance of these skills and abilities before?
3. How can chief information officers prepare their successors for an uncertain future that will most likely require skills different from those possessed by the successful CIOs of today? Which key competencies are enduring, and which ones are a function of the current technological environment? How can chief information officers prepare for the latter?

REAL WORLD ACTIVITIES

1. Go online to research the topic of executive succession planning and the different approaches in use by companies today. Are there any differences for those in information technology, as opposed to other functional areas, because of the dynamics of technology change and evolution? Which competencies are being targeted for IT executives? Prepare a report to summarize your findings.
2. The case mentions several strategies used by companies to mentor and develop their next generation of IT leaders: career planning, leadership development exercises, coaching, and so on. As a Generation Y member discussed in the chapter, how do these fit in with your expectations for the future? Break into small groups with your classmates to discuss these issues; in particular, to what extent you believe these approaches match well with your culture and personality?

REAL WORLD CASE 4

Reinsurance Group of America and Fonterra: Going for Unified Global Operations

LUTTRELL, SONYA LOUISE 256668U

The reinsurance industry isn't for the faint of heart. The business processes that enable reinsurance firms to form agreements with other insurance companies to accept all or part of their risk can get mighty complex, mighty quickly.

Now imagine developing a single system that manages reinsurance business processes for numerous offices around the world—offices whose staffs speak different languages, are in different time zones, and just might be stuck in their ways as to how they manage their business. It's a challenge that could overwhelm you if you tried to tackle it all at once instead of breaking it into small pieces.

When workers in the global software group at Reinsurance Group of America Inc. (RGA) in Chesterfield, Missouri, first took on this mammoth project, they would have been the first to tell you they were unprepared for the obstacles that lay ahead.

"This whole system required so much communication and teamwork, and I'm not sure we understood at first what we needed to contribute to make it a success," says Mike Ring, project manager at RGA. Yet by engaging the business and adapting its own practices to the demands of the situation, the group is successfully rolling out an integrated, multicurrency, multilanguage life reinsurance administration system, dubbed CybeRe, for its international division.

Before CybeRe, workers in RGA's global offices mainly relied on a mix of spreadsheets and databases to manage clients. Now, with information stored in one location, workers can analyze data by client, contract, and product and find client errors more easily. "People can stop worrying about, 'If I sell this business, how am I going to manage it?'" says Azam Mirza, vice president of global software and head of the CybeRe effort.

The system also strengthens data validation and data quality, Ring adds, which will enable better risk analysis and retention analysis, resulting in better profitability. Ultimately, return on investment will reach more than 15 percent, "which compares very favorably to the average ROI for RGA's products, which are normally in the range of 12 percent to 15 percent," Mirza says.

The picture wasn't always this rosy. When the project began six years ago, IT began to gather business requirements from the global offices, planning to emerge a couple of years later with a full-blown system. By late 2001, however, it became apparent that a phased approach was more practical. "The different units all do things slightly differently, and getting everyone to agree became very contentious," explains Kam Chan, chief architect of CybeRe. So the group embarked on a plan to build a pilot system in one office (South Africa) and gradually implement it in the remaining ones, with as few customizations as possible.

It wasn't always smooth sailing. For one thing, converting all the historical data and loading it into the CybeRe system required a significant data cleansing and migration effort. Other factors, such as differences in the terminologies used in various offices, also caused delays. For example, while it gathered requirements, IT asked whether the South African office used compound benefits. Although it said it did not, it turned out that the office just used a different term: acceleration of benefits.

"The change in scope delayed us four or five months," Mirza says. Probably the biggest challenge—which continues today—is getting people to accept common practices as defined by the system. "That's where we're the bad guys," Mirza says. "If they really need it, they have to prove it. We challenge everything. We don't want to create a product that's convoluted because it tries to be everything to everybody."

Despite the local customizations, RGA still maintains just one version of CybeRe. Local units can just "turn on" the options or customizations that are relevant to their businesses. "Not maintaining 13 different versions is very important," Mirza says. "It's critical to our success."

"Given the life reinsurance market's consolidation of recent years, CybeRe should provide RGA with an important competitive weapon. RGA aims to 'reinvent reinsurance.' That is an ambitious goal. CybeRe is an important step along the way."

Greg James is chief information officer and general manager of global business processes at Fonterra. It is a unique role, instrumental in ensuring that the only silos at the dairy group are of the giant stainless steel variety. James was on sabbatical following a year-long assignment in Europe with the New Zealand Dairy Board when he was offered to head what he describes as a "small business initiative" called Jedi. The call came from an executive of Fonterra, which had just been formed, and the job was director of the dairy group's biggest business transformation program to date.

Jedi, which was rolled out in 2.5 years, entailed moving Fonterra's commodity business to a common ERP platform and "a single global way of doing things." James says the Jedi program aimed to look at the supply chain of the dairy giant "from cow to manufacturing to storage to happy customers."

The change involved was massive, for Fonterra's supply chain covers four million cows that produce 20 billion liters of milk each year. It has offices in 70 countries and employs nearly 19,000 staff. Fonterra, says James, would be recognized as New Zealand's largest company if it were listed in the Stock Exchange. In order to implement the new environment, "We had to reinvent ourselves; analyze every part of the business, all processes, all organizational structure," says James.

In effect, the Jedi program dismantled traditional silos in the organization and standardized global processes. "It has enabled us to effectively bring all components that previously existed in each group, in other business units, bring them all together and get commonality in terms of the way

we do things. It has driven consistency of processes, and has enabled us to draw consistency in approaching framework in terms of how we operate."

Today, he notes, "We do the things the same way in Germany, Mexico and New Zealand." As James explains, Fonterra was set up in 2000 as an amalgamation of the old dairy industry, with self-contained business functions. Fonterra consolidated its back-office functions globally within New Zealand, into a business transactional services activity based in Hamilton. James says the Hamilton operations fared well when benchmarked against BPO organizations locally and overseas. "Our model is better than most international models." Instead of having disparate sales offices for various business units, a customer service center was set up at the Auckland's Princes Street headquarters. This center operates around the clock, providing multilingual support for customers across the globe.

For Fonterra's 200-member IS team, the new system means being exposed to areas of the business they traditionally would not have been. "If they worked in this part of the business under the old structure, they tended to stay in that part of the business.

But now we pool the resources together so it means they could be working on X, Y, or Z within any given period. They are given a lot more flexibility and ability to learn the various parts of the business in the new model."

He believes this setup also helps in staff retention. "It does give us the ability to retain staff as opposed to having staff leave to go to other organizations to experience different types of skill sets." If there is another thing James is empathic about, it is that these days at Fonterra, "There is no such thing as an IT project by itself."

"We sit down with the business in terms of our planning, and we align our plans to their plans." He says there is now an "enterprise road map" that consists of all the activities the business wants to undertake over the next 18 months up to three years.

What is his primary advice for IT professionals who wish to move on to chief information officer and other C-level roles? "Make sure that you understand the business that you work with." He adds, "Keep a watchful eye on very, very competent people that you might need to hire one day to be part of a bigger team." They could be people in your current organization or people you meet outside, in industry functions.

Lastly, he says, "Never ever fear hiring someone in your organization that is smarter than you. You actually need a lot of smart people working around you."

Source: Adapted from Mary Brandel, "Reinsurance Group Simplifies on Global Scale with Administration System," *Computerworld*, March 14, 2005; and Divina Paredes, "Unifying Global Operations," *CIO Magazine*, March 27, 2007.

CASE STUDY QUESTIONS

1. What is the business value of these global system developments for the companies mentioned in the case? How did they achieve these benefits? What were the major obstacles they had to overcome?
2. What are the advantages and disadvantages of a full-blown versus a phased approach for system implementations in general, and global ones in particular? How do you make the decision on which road to take?
3. How important is it that all units in global organization speak the same business language, and use the same functions and business processes? How do you balance the competing needs for flexibility and consistency across operations?

REAL WORLD ACTIVITIES

1. Both organizations featured in the case have been quite successful with their global rollouts. Search the Internet for examples of less-than-thriving global or international system implementations. How do they compare to the ones in the case? What differences in the approaches taken by the successful and unsuccessful cases do you think could account for the differences in outcome? Prepare a report and a presentation to share your findings with the rest of the class.
2. Implementing major systems in global organizations, particularly when development is concentrated in headquarters or a powerful country subsidiary, can cause a lot of resentment and frustration for the other units in the organization. Break into small groups with your classmates to discuss which approaches companies can take to ease these issues and incorporate all of their units into the process.