The IBM mainframe couldn't handle the application, so the school was forced to purchase a UNIX system. Vice president of Human Resources Joseph Nolan claimed that 35 functions the software was supposed to perform were either missing or did not work. University officials say that the system failed to process financial aid and sent out incorrect tuition bills, a mistake that hit Cleveland State with a $5 million loss. The university hired new consultants, spent an additional $7 million, and installed hundreds of fixes, but the system still didn't work as promised.

In January 2004, Cleveland State finally threw up its hands and filed a $510 million lawsuit against PeopleSoft for breach of contract, fraud, and negligent misrepresentation. The university also sued Klaudis. After Oracle acquired PeopleSoft, both parties agreed to a settlement of $4.25 million. Although the university has not recovered its losses, it has served as a cautionary tale for others.[1,2,3,4,5,6]

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key characteristics distinguish a professional from other kinds of workers, and what is the role of an IT professional?
2. What relationships must an IT professional manage, and what key ethical issues can arise in each?
3. How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
4. What are the key tenets of four different codes of ethics that provide guidance for IT professionals?
5. What are the common ethical issues that face IT users?
6. What approaches can support the ethical practices of IT users?

IT PROFESSIONALS

A profession is a calling that requires specialized knowledge and often long and intensive academic preparation. The United States has adopted labor laws and regulations that require a more precise definition of what is meant by a *professional* employee. The U.S. Code of Federal Regulations defines a person "employed in a professional capacity" as one who meets these four criteria:

1. One's primary duties consist of the performance of work requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study or work.
2. One's instruction, study, or work is original and creative in character in a recognized field of artistic endeavor and the result of which depends primarily on the invention, imagination, or talent of the employee.
3. One's work requires the consistent exercise of discretion and judgment in its performance.
4. One's work is predominately intellectual and varied in character, and the output or result cannot be standardized in relation to a given period of time.

In other words, professionals such as doctors, lawyers, and accountants require advanced training and experience, they must exercise discretion and judgment in the course of their work, and their work cannot be standardized. Many people would also expect professionals to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in their field, and to help develop other professionals. In addition, many professional roles carry special rights and special responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information.

Are IT Workers Professionals?

Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists. A partial list of IT specialists includes programmers, systems analysts, software engineers, database administrators, local area network (LAN) administrators, and chief information officers (CIOs). One could argue, however, that not every IT role requires "knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study," to quote again from the U.S. Code's definition of a professional. From a legal perspective, IT workers are not recognized as professionals because they are not licensed. This distinction is important, for example, in malpractice lawsuits—many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.

Professional Relationships That Must Be Managed

IT professionals typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large. In each relationship, an ethical IT professional acts honestly and appropriately. These various relationships are discussed in the following sections.

Relationships Between IT Professionals and Employers

IT professionals and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT professional and employer discuss and agree upon fundamental aspects of this relationship before the professional accepts an employment offer. These issues include job title, general performance expectations, specific work responsibilities, drug testing, dress code, location of employment, salary, work hours, and company benefits. Many other issues are addressed in the company's policy and procedures manual or in the company code of conduct, if it exists; these issues include protection of company secrets, vacation policy, time off for a funeral or illness in the family, tuition reimbursement, and use of company resources, including computers and networks. Other aspects of the relationship develop over time as the need arises (for example, whether the employee can leave early one day if the time is made up on another day). Some aspects are addressed by law—for example, an employee cannot be required to do anything illegal, such as falsify the results of a quality assurance test. Some aspects are specific to the role of the IT professional and are established based on the nature of the work or project—for example, the programming language to be used, the type and amount of documentation to be produced, and the extent of testing to be conducted.

As the stewards of an organization's IT resources, IT professionals must set an example and enforce policies regarding the ethical use of IT. IT professionals have the skills and knowledge to abuse systems and data or to allow others to do so. **Software piracy**, the act of illegally making copies of software or enabling others to access software to which they are not entitled, is an area in which IT professionals can be tempted to violate laws and policies. Although end users get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to IT staff—either they allow it to happen or actively engage in it, often to reduce IT-related spending to meet challenging budgets. According to a study conducted by International Data Corporation (IDC), a global provider of market intelligence, advisory services, and events for the IT and telecommunications industries, 35 percent of the world's software was illegally copied in 2004. This represents a 1 percent decrease from 2003. Yet, losses due to piracy increased from $29 billion to $33 billion. Table 2-1 lists the 10 countries that had the highest software piracy rates in 2004 and the 10 countries with the lowest rates.[7]

The Business Software Alliance (BSA) is a trade group that represents the world's largest software and hardware manufacturers. Its mission is to stop the unauthorized copying of software produced by its members (see Table 2-2). More than 100 BSA lawyers and investigators prosecute thousands of cases of software piracy each year.[8] BSA investigations are usually triggered by calls to the BSA hotline (888-NO-PIRACY), reports sent to the BSA Web site, and referrals from member companies. Many of these cases are reported by disgruntled employees. When the BSA finds cases of software piracy, it assesses heavy monetary penalties. BSA is funded through dues based on member companies' software revenues and through settlements from companies that commit piracy. In 2004, for example, Red Bull North America Inc. paid the BSA $105,000 to settle claims that it had more copies of Adobe, Microsoft, and Symantec software programs on its computers than it had licenses to support.

Failure to cooperate with the BSA can be extremely expensive. The cost of criminal or civil penalties to a corporation and the people involved can easily be many times more expensive than the cost of "getting legal" by acquiring the correct number of software licenses. Penalties can be up to $100,000 per copyrighted work if a software piracy case goes to trial and the defendant loses.

TABLE 2-1 Software piracy rates of selected countries

10 countries with the highest piracy rates	2004 piracy rate	10 countries with the lowest piracy rates	2004 piracy rate
Vietnam	92%	United States	21%
Ukraine	91%	New Zealand	23%
China	90%	Austria	25%
Zimbabwe	90%	Sweden	26%
Indonesia	87%	United Kingdom	27%
Russia	87%	Denmark	27%
Nigeria	84%	Switzerland	28%
Tunisia	84%	Japan	28%
Algeria	83%	Finland	29%
Kenya	83%	Germany	29%

TABLE 2-2 Members of Business Software Alliance (as of July 2005)

Adobe	Apple	Autodesk
Avid	Bentley Systems	Borland
Cadence	Cisco Systems	CNC Software/Mastercam
Dell	Entrust	HP (Hewlett-Packard)
IBM	Intel	Internet Security Systems
Macromedia	McAfee, Inc.	Microsoft
PTC	RSA Security	SAP
SolidWorks	Sybase	Symantec
The Mathworks	UGS Corp.	VERITAS Software

Trade secrecy is another area that can cause problems between employers and IT professionals. A trade secret is information used in a business, generally unknown to the public, that the company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and has some degree of uniqueness or novelty. Trade secrets can include the design of new software code, hardware designs, business plans, the design of the user interface to a computer program, and manufacturing processes. Examples include the Colonel's secret recipe of 11 herbs and spices, the formula for Coke, and Intel's manufacturing process for the Pentium 4 chip. Employers fear that employees may reveal these secrets to competitors, especially when they leave the company. As a result, they require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets. However, the IT industry is known for high employee turnover, and things can get complicated when an employee moves on to a competitor.

In 2005, for example, a California jury ordered Toshiba Corporation to pay $465 million in damages to Lexar, its former business partner, for theft of trade secrets. The case centered on technology used in flash memory chips, which are widely used in computers and other consumer products to retain data when their power supply is disconnected. Lexar is a manufacturer and marketer of removable flash memory cards, USB flash drives (see Figure 2-1), card readers, and controller technology solutions for the digital photography, consumer electronics, and communications markets. Lexar sued Toshiba because it used its relationship to gain access to Lexar's business plans and technology while simultaneously working with SanDisk Corporation, a major rival of Lexar, on similar flash memory technology, according to Lexar spokespeople. In addition, Lexar asked for an injunction that bars Toshiba products from sale in the United States if they include the Lexar technology.[9]

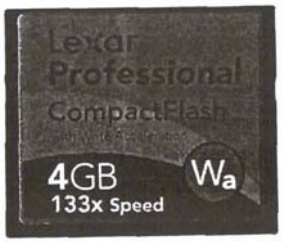

FIGURE 2-1 Lexar flash memory products

Another issue that can create friction between employers and IT professionals is whistle-blowing. Whistle-blowing is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. Whistle-blowers often have special information based on their expertise or position within the offending organization. For example, an employee of a chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee could then consider becoming a whistle-blower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, and could even result in retaliation and firing.

In May 2005, for example, Oracle Corporation paid $8 million to settle charges that it fraudulently collected fees before providing training for clients and failed to comply with federal travel regulations in billing for travel and expenses. The charges arose from a whistle-blower lawsuit brought by a former Oracle vice president. As a result of the settlement, the whistle-blower received $1.58 million of the $8 million total settlement.[10] Whistle-blowing is discussed more fully in Chapter 8.

Relationships Between IT Professionals and Clients

A professional often provides services to clients who either work outside the professional's organization or are "internal." In relationships between IT professionals and clients, each party agrees to provide something of value to the other. Generally speaking, the IT professional provides hardware, software, or services at a certain cost and within a given time frame. For example, an IT professional might agree to implement a new accounts payable software package that meets the client's requirements. The client provides compensation, access to key contacts, and perhaps work space. This relationship is usually documented in contractual terms—who does what, when the work begins, how long it will take, how much the client pays, and so on. Although there is often a vast disparity in expertise between IT professionals and their clients, the two parties must work together to be successful.

Typically, the client makes decisions about a project on the basis of information, alternatives, and recommendations provided by IT professionals. The client trusts them to use their expertise and to think and act in the client's best interests. The IT professional must trust that the client will provide relevant information, listen to and understand what the professional says, ask questions to understand the impact of key decisions, and use the information to make wise choices between alternatives. Thus, the responsibility for decision making is shared between client and professional.

One ethical problem between IT professionals and clients involves IT consultants or auditors who recommend their own products and services or those of an affiliated vendor to remedy a problem they have detected. For example, an IT consulting firm might be hired to assess a firm's IT strategic plan. After a few weeks of analysis, the consulting firm might provide a poor rating for the existing strategy and insist that its proprietary products and services are required to develop a new strategic plan. Such findings raise questions about the vendor's objectivity and whether its recommendations can be trusted.

During a project, IT professionals might be unable to provide full and accurate reporting of the project's status if they lack the information, tools, or experience to perform an accurate assessment. The project manager may want to keep resources flowing into the project and hope that problems can be corrected before anyone notices. The project manager may also be reluctant to share status information because of contractual penalties for failure to meet the schedule or to develop certain system functions. In this situation, the client may not be informed about the problem until it has become a crisis. After the truth comes out, finger-pointing and heated discussions about cost overruns, missed schedules, and technical incompetence can lead to charges of fraud, misrepresentation, and breach of contract, as discussed in the following Legal Overview.

LEGAL OVERVIEW

Fraud, Misrepresentation, and Breach of Contract

Fraud is the crime of obtaining goods, services, or property through deception or trickery. Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on the misrepresentation. To prove fraud in a court of law, prosecutors must demonstrate the following elements:

1. The wrongdoer made a false representation of material fact.
2. The wrongdoer intended to deceive the innocent party.
3. The innocent party justifiably relied on the misrepresentation.
4. The innocent party was injured.[11]

Breach of contract occurs when one party fails to meet the terms of a contract. Further, a material breach of contract occurs when a party fails to perform certain express or implied obligations that impair or destroy the essence of the contract. Because there is no clear line between a minor breach and a material breach, determination is made on a case-by-case basis.[12] "When there has been a material breach of contract, the nonbreaching party can either: (1) rescind the contract, seek restitution of any compensation paid under the contract to the breaching party, and be discharged from any further performance under the contract; or (2) treat the contract as being in effect and sue the breaching party to recover damages."[13]

When IT projects go wrong because of cost overruns, schedule slippage, lack of system functionality, and so on, aggrieved parties might charge fraud, fraudulent misrepresentation, and/or breach of contract. Trials can take years to settle, generate substantial legal fees, and create bad publicity for both parties. As a result, more than 90 percent of such disputes are settled out of court, and the proceedings and outcomes are concealed from the public. In addition, IT vendors have become more careful about protecting themselves from major legal losses by requiring that contracts place a limit on potential damages.

Most IT projects are joint efforts in which vendors and customers work together to develop a system. Assigning fault when such projects go wrong can be difficult; one side might be partially at fault while the other side is mostly at fault. Consider the following frequent causes of problems in IT projects:

- The customer changes the scope of the project or the system requirements during the effort.
- Poor communications between customer and vendor lead to performance that does not meet expectations.
- The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- The customer fails to reveal information about legacy systems or databases that make the new system extremely difficult to implement.

continued

Who is to blame in such circumstances? For example, Collin County, Texas, awarded an $8 million contract to Siemens Business Services Inc. for software applications to manage the fast-growing county's financial, human resources, and other operations. Shortly after work began, however, Siemens encountered problems meeting the contract's requirements. Eventually, Siemens said it couldn't complete the project at all. Angry county leaders sued Siemens and the software vendor's public-services unit for $10 million for fraud and breach of contract after having paid $1 million for previous work.[14]

Relationships Between IT Professionals and Suppliers

IT professionals deal with many different hardware, software, and service providers. Most IT professionals understand that building a good working relationship with suppliers encourages the flow of useful communication and the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier's products and services that the IT professional may never have considered.

IT professionals should develop good relationships with suppliers by dealing fairly with them and not making unreasonable demands. Threatening to replace a supplier who can't deliver needed equipment tomorrow, when the normal industry lead time is one week, is aggressive behavior that does not help a working relationship.

Suppliers also strive to maintain positive relationships with their customers to make and increase sales. Sometimes, their actions to achieve this goal might be perceived as unethical—for example, they could offer an IT professional a gift that is actually intended as a bribe. Clearly, IT professionals should not accept a bribe from a vendor, but they must be careful in considering what constitutes a bribe. For example, accepting invitations to expensive dinners or payment of entry fees for a golf tournament may seem innocent to the recipient, but may be perceived as bribery by an internal accounting auditor.

Bribery involves providing money, property, or favors to someone in business or government to obtain a business advantage. An obvious example is a software supplier that offers money to another company's employee to get its business. This type of bribe is often referred to as a "kickback" or "payoff." The person who offers a bribe commits a crime when the offer is made, and the recipient is guilty of bribery upon accepting the offer.

The U.S. Foreign Corrupt Practices Act (FCPA) makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office. The act applies to any U.S. citizen or company, or to any company with shares listed on any U.S. stock exchange. However, a bribe is not a crime if the payment was lawful under the laws of the foreign country in which it was paid. Penalties for violating the FCPA are severe—corporations face a fine of up to $2 million per violation, and individual violators may be fined up to $100,000 and imprisoned for up to five years.

The FCPA also requires corporations to meet its accounting standards by having an adequate system of internal controls, including maintaining books and records that accurately and fairly reflect their transactions. The goal of these standards is to prevent companies from using "slush funds" or other means to disguise payments to foreign officials. A firm's business practices and its accounting information systems are frequently audited both by internal and outside auditors to ensure that they meet these standards.

The FCPA permits facilitating payments that are made for "routine government actions," such as obtaining permits or licenses; processing visas; providing police protection; providing phone services, power, or water supplies; or facilitating actions of a similar nature. Thus, it is permissible under the FCPA to pay an official to perform some official function faster (for example, to speed customs clearance), but not to make a different substantive decision (for example, to award business to one's firm).

In some countries, gifts are an essential part of doing business. In fact, in some countries it would be considered rude not to bring a present to an initial business meeting. In the United States, a gift might take the form of free tickets to a sporting event from a personnel agency that wants to get on your company's list of preferred suppliers. At what point does a gift become a bribe? Who decides?

The key distinguishing factor is that no gift should be hidden. A gift may be considered a bribe if it is not declared. As a result, most companies require all gifts to be declared and that everything but token gifts must be declined. Some companies have a policy of pooling the gifts received by their employees, auctioning them, and giving the proceeds to charity.

When it comes to distinguishing between bribes and gifts, the perceptions of the donor and recipient can differ. The recipient may believe he received a gift that in no way obligates him to the donor, particularly if the gift was not cash. The donor's intentions, however, might be very different. Table 2-3 helps you distinguish between a gift and a bribe.

TABLE 2-3 Distinguishing between a bribe and a gift

Bribes	Gifts
Are made in secret, as they are neither legally nor morally acceptable	Are made openly and publicly as a gesture of friendship or goodwill
Are often made indirectly through a third party	Are made directly from donor to recipient
Encourage an obligation for the recipient to act favorably toward the donor	Come with no expectation of a future favor for the donor

Relationships Between IT Professionals and Other Professionals

Professionals feel a degree of loyalty to the other members of their profession. As a result, they are quick to help each other obtain new positions but slow to criticize each other in public. Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are perceived and treated. (For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the profession's code of conduct. Experienced professionals can also serve as mentors and help develop new members of the profession.

A number of ethical problems can arise between members of the IT profession. One of the most common is **résumé inflation**, which involves lying on a résumé and claiming competence in an IT skill that is in high demand. Even though IT professionals might benefit in the short term from exaggerating qualifications, such action can hurt the profession and themselves in the long run. Customers, and society in general, might become much more skeptical of IT professionals as a result. As many as 30 percent of job applicants exaggerate their accomplishments and about 10 percent seriously misrepresent their backgrounds, according to some estimates.[15]

Another ethical issue is the inappropriate sharing of corporate information. Because of their roles, IT professionals have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on. As discussed in Chapter 1, this information is sometimes shared inappropriately. It might be sold to other organizations or shared informally during work conversations with others who have no need to know.

Relationships Between IT Professionals and IT Users

The term **IT user** distinguishes the person for whom a hardware or software product is designed from the IT professionals who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

IT professionals have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs—subject, of course, to budget and time constraints. IT professionals also have a key responsibility to establish an environment that supports ethical behavior by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information. Later in this chapter, you will learn more about establishing an effective IT usage policy that addresses these issues.

Relationships Between IT Professionals and Society

Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they fail to safeguard against all negative side effects of a product or process. Often, professionals can see more clearly what effect their work will have and can take action to eliminate potential public risks. Thus, society not only expects members of a profession not to cause harm, but to provide significant benefits. One approach to meeting this expectation is to establish and maintain professional standards that protect the public.

Clearly, the actions of an IT professional can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process. A failure or error in the system may put workers or residents near the plant at risk. As a result, IT professionals have a relationship with others in society who may be affected by their actions. However, there is currently no single, formal organization of IT professionals that takes responsibility for establishing and maintaining standards that protect the public.

THE ETHICAL BEHAVIOR OF IT PROFESSIONALS

Chapter 1 points out that the risks associated with inappropriate ethical behavior have grown in number, complexity, likelihood, and significance. As a result, corporations are taking a number of actions to ensure good business ethics among their employees. This section focuses on actions that support the ethical behavior of IT professionals.

Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group. Practitioners in many professions subscribe to a code of ethics that governs their behavior. For example, doctors adhere to varying versions of the 2000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes. Most codes of ethics created by professional organizations have two main parts. The first outlines what the professional organization aspires to become, and the second typically lists rules and principles by which members of the organization are expected to abide. Many codes also include a commitment to continuing education for those who practice the profession. (For examples of professional codes of ethics, see Appendices B through E.)

Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean it is ethical. You also cannot expect a professional code of ethics to provide the complete answer—no code can be the definitive collection of behavioral standards. However, practicing according to a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

- *Improves ethical decision making*—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs to serve as a guideline for ethical decision making.
  Promotes high standards of practice and ethical behavior—Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business. The code also defines behaviors that are acceptable and unacceptable to guide professionals in their interactions with others. Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few of them exist in the IT arena.
  Enhances trust and respect from the general public—Public trust is built on the expectation that a professional will behave ethically. People often must depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions. Thus, adherence to a code of ethics enhances trust and respect of professionals and their profession.
- *Provides an evaluation benchmark*—A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

Professional Organizations

No IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT professionals. However, the existence of such organizations is useful in a field that is rapidly growing and changing. IT professionals need to know about new developments in the field, which requires networking with others, seeking out new ideas, and building personal skills and expertise. Whether you are a freelance programmer or the CIO of a Fortune 500 company, membership in an organization of IT professionals enables you to associate with others of similar work experience, to develop working relationships, and to exchange ideas. Information is disseminated from these organizations through e-mail, periodicals, Web sites, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed a code of ethics. Four of the most prominent IT-related professional organizations are summarized in this section.

Association for Computing Machinery (ACM)

The ACM is a computing society founded in 1947 that serves more than 80,000 professionals in more than 100 countries and offers many publications for technology professionals. *Tech News*, for example, is a comprehensive news-gathering service published three times a week. ACM's *Ubiquity* publication is a forum and opinion magazine. The organization also offers a substantial digital library of bibliographic information, citations, articles, and journals. The ACM sponsors special-interest groups that focus on a variety of IT issues, including artificial intelligence, computer architecture, programming languages, computer-human interaction, and mobile communications. Each group provides publications, workshops, and conferences for information exchange.

The ACM has a code of ethics and professional conduct with supplemental explanations and guidelines. The ACM code consists of eight general moral imperatives, eight specific professional responsibilities, six organizational leadership imperatives, and two elements of compliance. The complete text of this code is provided in Appendix B.

Association of Information Technology Professionals (AITP)

The AITP has its roots in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the TAB machines they were operating. They were members of a local group called the Machine Accountants Association (MAA), which evolved into the Data Processing Management Association in 1962 and finally the AITP in 1996.

The AITP provides quality IT-related education, information on relevant IT issues, and forums for networking with experienced peers and other IT professionals for its nearly 9000 members.[16] Its mission is to provide superior leadership and education in information technology, and one of its goals is to help members make themselves more marketable to the industry. The AITP also has a code of ethics and standards of conduct, which are presented in Appendix C. The standards of conduct are considered to be rules that no true IT professional should violate.

Computer Society of the Institute of Electrical and Electronics Engineers (IEEE-CS)

The Institute of Electrical and Electronics Engineers (IEEE) covers the broad fields of electrical, electronic, and information technologies and sciences. The IEEE-CS is one of the oldest and largest IT professional associations, with more than 100,000 members. Roughly 40 percent of its members live and work outside the United States. Founded in 1946, the IEEE-CS is the largest of the 36 societies of the IEEE. "The IEEE-CS's vision is to be the leading provider of technical information and services to the world's computing professionals. The society promotes an active exchange of information, ideas, and technological innovation among its members through its many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups."[17]

In 1993, the IEEE-CS and the ACM formed a Joint Steering Committee for the Establishment of Software Engineering as a Profession. The initial recommendations of the committee were to define ethical standards, to define the required body of knowledge and recommended practices in software engineering, and to define appropriate curricula to acquire knowledge. The Software Engineering Code of Ethics and Professional Practice (see Appendix D) documents the ethical and professional responsibilities and obligations of software engineers.

Project Management Institute (PMI)

The Project Management Institute was established in 1969 and currently has more than 150,000 members in more than 150 countries. Its members include project managers from such diverse fields as construction, sales, finance, and production, not just information systems. It has certified more than 100,000 people as project management professionals (PMPs). Certification requires that a person meet specific education and experience requirements, agree to follow the PMP Code of Ethics, and pass the PMP exam, which is designed to assess and measure knowledge of project management. The PMI Member Code of Ethics is presented in Appendix E.

Certification

Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Unlike licensing, which applies only to people and is required by law, certification can also apply to products and is generally voluntary. IT-related certifications typically carry no requirement to adhere to a code of ethics, whereas such a requirement is standard with licensing.

Numerous companies and professional organizations offer certifications, and opinions are divided on their value. Many employers view them as a benchmark that indicates mastery of a defined set of basic knowledge. On the other hand, because certification is no substitute for experience and doesn't guarantee that a person will perform well on the job, some hiring managers are rather cynical on the subject. Most IT employees are motivated to learn new skills, and certification provides a structured way of doing so. For such people, completing a certification provides clear recognition and correlates with a good plan to help them advance their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.[18]

Vendor Certifications

Many IT vendors such as Cisco, IBM, Microsoft, Sun, and Oracle offer certification programs for their products. Workers who successfully complete a program can represent themselves as certified users of a manufacturer's product. Depending on the job market and the demand for skilled workers, some certifications might substantially improve IT workers' salaries and career prospects. Certifications that are tied to a vendor's product are relevant for narrowly defined roles or certain aspects of broader roles. Sometimes, however, vendor certifications are too focused on technical details and do not address more general concepts.

Certifications require passing a written exam, which usually contains multiple-choice questions because of legal concerns about whether other types of exams can be graded objectively. A few certifications, such as Cisco Certified Internetworking Engineer (CCIE), also require a hands-on lab exam that demonstrates skills and knowledge. It can take years to obtain the necessary experience required for some certifications. Courses and training material are available to help speed up the preparation process, but some training costs can be expensive. Depending on the certification, study materials can cost $1000 and in-class formal training courses can cost more than $10,000.

The Microsoft Certified System Engineer (MCSE) certification is one of the more demanding Microsoft certifications. Engineers, analysts, and consultants frequently obtain it for their work in designing and implementing Windows server solutions and architectures. Four networking system exams, one client operating system exam, and one design exam are required. So many people have obtained MCSE certification (more than 400,000 in the United States) that it has almost become an entry-level requirement for some companies.

Because of the rapid pace of change in the IT field, workers are commonly recertified as newer technologies become available. For example, many people who were MCSE-certified and trained on the Windows NT 4.0 operating system went through recertification when newer operating systems were developed.

Industry Association Certifications

Certifications from industry associations generally require a certain level of experience and a broader perspective than vendor certifications; however, they often lag in developing tests that cover new technologies. The trend in IT certification is to move from purely technical content to a broader mix of technical, business, and behavioral competencies, which are required in today's demanding IT roles. This trend is evident in industry association certifications that address broader roles such as e-commerce, network security, and project management.

For example, the Institute for Certification of Computing Professionals (ICCP) offers two levels of certification—Certified Associate Computing Professional and Certified Computing Professional. Since 1973, more than 50,000 IT professionals worldwide have completed ICCP certification.[19] Candidates for either certificate must take a common core exam that includes questions on organizational frameworks, systems concepts, data and information, systems development, technology, and associated disciplines.

The Associate Computing Professional (ACP) certification requires applicants to successfully complete an exam for an additional computer programming language. The ACP certification is for new members of the IT industry or recent college graduates who want professional credentials that substantiate their level of computing knowledge.

More experienced IT professionals can obtain the Certified Computing Professional (CCP) certification, which requires successful completion of exams in two of the following areas: management, procedural programming, business information systems, communications, office information systems, systems security, microcomputing and networks, systems development, software engineering, systems programming, and data resource management. In addition, CCP candidates must have four years of full-time experience in information systems or applicable college degrees with two years of full-time experience. All candidates must subscribe to a specified code of ethics, conduct, and good practice.[20]

The American Society for Quality Control (ASQC) offers certifications for software quality engineers who have eight years of professional experience and at least three years in a decision-making position. A bachelor's degree may count as four years of experience, and an advanced degree may count as an additional, fifth year of experience. In addition, engineers must have professional credentials, such as membership in a recognized professional society, an engineer's license, or statements from two professional colleagues. Engineers must successfully complete a written exam that covers software quality management, software engineering, project management, analytical methods, and quality systems.

Clearly, many IT certifications are available. Their value varies greatly depending on where people are in their career path, what other certifications they possess, and the nature of the IT job market.

Government Licensing

Government licensing is generally administered at the state level in the United States. Some professionals must be licensed to prove that they can do their work ethically and safely, including certified public accountants (CPAs), lawyers, doctors, various types of medical and day care providers, and some engineers.

Various states have enacted legislation to establish licensing requirements and protect public safety. For example, Texas passed the Engineering Registration Act after a tragic school explosion at New London, Texas, in 1937. Under the act and subsequent revisions, only duly licensed people may legally perform engineering services for the public, and public works must be designed and constructed under the direct supervision of a licensed professional engineer. People cannot call themselves engineers or professional engineers unless they are licensed, and violators are subject to legal penalties.[21] Most states have similar laws.

The Case for Licensing IT Professionals

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on each other. Highly integrated enterprise resource planning systems (ERPs) help multibillion-dollar companies control all their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution. Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity for cities. Medical information systems monitor the vital statistics of hospital patients on critical life support. Local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern. This concern has led to a debate whether the licensing of IT professionals would improve information systems. Proponents argue that licensing would strongly encourage IT professionals to follow the highest standards of the profession and practice a code of ethics, and that licensing would allow violators to be punished. Without licensing, there are no requirements for heightened care and no concept of professional malpractice.

Issues Associated with Government Licensing of IT Professionals

Australia, Great Britain, and the Canadian provinces of Ontario and British Columbia have adopted licensing for software engineers. The National Council of Engineering Examiners and Surveyors (NCEES) has developed a professional exam for electrical engineers and computer engineers.[22] However, there are few international or national licensing programs for IT professionals, for many reasons:

- *There is no universally accepted core body of knowledge.* The core body of knowledge for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. At present, however, there are no universally accepted standards for licensing programmers, software engineers, and other IT professionals. Instead, various professional societies, state agencies, and federal governments have developed their own standards.
- *It is unclear who should manage the content and administration of licensing exams.* How will licensing exams be constructed, and who will be responsible for designing and administering them? Will someone who passes a license exam in one state or country be accepted in another state or country? In a field as rapidly changing as IT, professionals clearly must commit to ongoing, continuous education. If an IT professional's license expires every few years (like a driver's license), when must practitioners prove competence in new practices before they can renew their license? Such questions would normally be answered by the state agency that licenses other professionals.
- *There is no administrative body to accredit professional education programs.* Unlike the American Medical Association for medical schools or the American Bar Association for law schools, no single body accredits IT professional education programs. Furthermore, there is no well-defined, step-by-step process to train IT professionals, even for specific jobs, such as programming. There is not even broad agreement on what skills a good programmer must possess—it is highly situational, depending on the computing environment.
- *There is no administrative body to assess and ensure competence of individual professionals.* Lawyers, doctors, and other licensed professionals

are held accountable to high ethical standards and can lose their license for failing to meet these standards or for demonstrating incompetence. The AITP standards of conduct state that professionals should "take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest." The AITP code addresses the censure issue much more forcefully than other IT codes of ethics, although it has seldom, if ever, been used to censure practicing IT professionals.

IT PROFESSIONAL MALPRACTICE

Negligence has been defined as not doing something that a reasonable man would do, or doing something that a reasonable man would not do. **Duty of care** refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely. Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions for employees.

The courts decide whether parties owe a duty of care by applying a **reasonable person standard** to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances. Likewise, defendants who have particular expertise or competence are measured against a **reasonable professional standard**. For example, in a medical malpractice suit based on improper treatment of a broken bone, the reasonable person standard would be higher if the plaintiff were an orthopedic surgeon rather than a general practitioner. In the IT arena, consider a negligence case in which an employee inadvertently destroyed millions of customer records. The reasonable person standard would be higher if the plaintiff were a licensed, Oracle-certified database administrator (DBA) with 10 years of experience, instead of an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle system.

If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached. A **breach of the duty of care** is the failure to act as a reasonable person would act. A breach of duty may consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer who does not protect a citizen from an attacker.

Professionals who breach this duty of care are liable for injuries their negligence causes. This liability is commonly referred to as **professional malpractice**. For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice. Professionals who breach this duty are liable to their patients or clients, and possibly to some third parties.

Courts have consistently rejected attempts to sue individual parties for computer-related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States. Because there are no uniform standards against which to compare a software engineer's professional behavior, he cannot be subject to malpractice lawsuits.

IT USERS

Chapter 1 outlined the general topic of how corporations are addressing the increasing risks of unethical behavior. This section focuses on improving employees' ethical use of IT, which has become an area of growing concern as more companies provide employees with PCs, access to corporate information systems and data, and the Internet.

Common Ethical Issues for IT Users

This section discusses a few common ethical issues for IT users. Other ethical issues will be discussed in future chapters.

Software Piracy

As mentioned earlier in this chapter, software piracy in a corporate setting can be directly traceable to IT professionals—they might allow it to happen or they might actively engage in it. Corporate IT usage policies and management should encourage users to report instances of piracy and to challenge its practice.

Sometimes, IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home. When confronted, the IT user's argument might be: "I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work." However, this is still piracy if no one has paid for an additional license to use the software on the home computer.

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at worker productivity and waste time. Furthermore, viewing sexually explicit material, sharing lewd jokes, and sending hate e-mail could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment. According to a survey conducted by Delta Consulting in 2005, half of all Fortune 500 companies dealt with at least one incident related to computer porn in the workplace in the previous 12 months. The companies handled the problem by firing the offenders in 44 percent of the cases and taking other disciplinary action 41 percent of the time.[23]

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulae, tactical and strategic plans, and research and development. An IT user who shares this information with an unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors. For example, if an IT employee saw a coworker's payroll records and then discussed them with a friend, it would be a clear violation of the worker's privacy.

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems, so many organizations have recognized the need to develop policies that protect against abuses. Although no policy can stop wrongdoers, it can set forth the general rights and responsibilities of all IT users, establish boundaries of acceptable and unacceptable behavior, and enable management to punish violators. Adherence to the policy can improve services to users, increase productivity, and reduce costs. Companies can take several of the following actions when creating an IT usage policy.

Defining and Limiting the Appropriate Use of IT Resources

Companies must develop, communicate, and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance. Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Internet sites or using company e-mail to send offensive or harassing messages.

Establishing Guidelines for Use of Company Software

Company IT managers must provide clear rules that govern the use of home computers and associated software. Some companies negotiate contracts with software manufacturers and provide PCs and software so that IT users can work at home. Other companies help employees buy hardware and software at corporate discount rates. The goal should be to ensure that employees have legal copies of all the software they need to be effective, regardless of whether they work in an office, on the road, or at home.

Structuring Information Systems to Protect Data and Information

Organizations must implement systems and procedures that limit data access to employees who need it. For example, sales managers may have total access to sales and promotion databases through a company network, but their access should be limited to products for which they are responsible. Furthermore, they should be prohibited from accessing data about research and development results, product formulae, and staffing projections if they don't need it to do their jobs.

Installing and Maintaining a Corporate Firewall

A firewall is a hardware or software device that serves as a barrier between a company and the outside world and limits access to the company's network based on the organization's Internet usage policy. The firewall can be configured to serve as an effective deterrent to unauthorized Web surfing by blocking access to specific, objectionable Web sites. Unfortunately, the number of such sites grows so rapidly that it is difficult to block them all. The firewall can also serve as an effective barrier to incoming e-mail from certain Web sites, companies, or users. It can even be programmed to block e-mail with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

Table 2-4 presents a manager's checklist that summarizes items to consider when establishing an IT usage policy. The preferred answer in each case is *yes*.

TABLE 2-4 Manager's checklist of items to consider when establishing an IT usage policy

Questions	Yes	No
Is there a statement that explains the need for an IT usage policy?	___	___
Does the policy provide a clear set of guiding principles for ethical decision making?	___	___
Is it clear how the policy applies to the following types of workers?		
Employees	___	___
Part-time workers	___	___
Temps	___	___
Contractors	___	___
Does the policy address the following issues?		
Protection of the data privacy rights of employees, customers, suppliers, and others	___	___
Limits and control of access to proprietary company data and information	___	___
The use of unauthorized or pirated software	___	___
Employee monitoring, including e-mail, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video	___	___
Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks	___	___
Inappropriate use of IT resources, such as Web surfing, e-mailing, and other use of computers for purposes other than business	___	___
The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, use of "hard-to-guess" passwords, and frequent changing of passwords	___	___
The use of the computer to intimidate, harass, or insult others through abusive language in e-mails and by other means	___	___
Are disciplinary actions defined for IT-related abuses?	___	___
Is there a process for communicating the policy to employees?	___	___
Is there a plan to provide effective, ongoing training relative to the policy?	___	___
Has a corporate firewall been implemented?	___	___
Is the corporate firewall maintained?	___	___

Summary

1. What key characteristics distinguish a professional from other kinds of workers, and what is the role of an IT professional?

   Professionals require advanced training and experience, they must exercise discretion and judgment in the course of their work, and their work cannot be standardized. A professional is expected to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in the field, and to help develop other professionals. From a legal standpoint, a professional has passed the state licensing requirements (if they exist) and earned the right to practice there.

2. What relationships must an IT professional manage, and what key ethical issues can arise in each?

   IT professionals typically become involved in many different relationships, each with its own set of ethical issues and potential problems. In relationships between IT professionals and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets. In relationships between IT professionals and clients, the key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. A major goal for IT professionals and suppliers is to develop good working relationships in which no action can be perceived as unethical. In relationships between fellow IT professionals, the key issues are to improve the profession through such activities as mentoring inexperienced colleagues and demonstrating professional loyalty. Résumé inflation and the inappropriate sharing of corporate information are relevant problems. In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information. When it comes to the relationship between IT professionals and society at large, the main challenge is to practice the profession in ways that cause no harm to society and provide significant benefits.

3. How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?

   A professional code of ethics states the principles and core values that are essential to the work of an occupational group. A code serves as a guideline for ethical decision making, promotes high standards of practice and ethical behavior, enhances trust and respect from the general public, and provides an evaluation benchmark.

   Many people believe that the licensing and certification of IT professionals would increase the reliability and effectiveness of information systems, but the question of licensing raises many issues; for example, (a) there is no universally accepted core body of knowledge on which to test people; (b) it is unclear who should manage the content and administration of licensing exams; (c) there is no administrative body to accredit professional education programs; and (d) there is no administrative body to assess and ensure competence of individual professionals.

4. What are the key tenets of four different codes of ethics that provide guidance for IT professionals?

   Several IT-related professional organizations have developed a code of ethics, including the ACM, the AITP, the IEEE-CS, and the Project Management Institute. These codes have two main parts—the first outlines what the organization aspires to become, and the second typically lists rules and principles that members are expected to live by. They also include a commitment to continuing education for those who practice the profession.

5. What are the common ethical issues that face IT users?

   Issues include software piracy, inappropriate use of corporate IT resources, and the inappropriate sharing of private and secret information.

6. What approaches can support the ethical practices of IT users?

   The development of an IT usage policy is the first step for an organization in defining appropriate and inappropriate IT user behavior. The policy should define and limit the appropriate use of IT resources and set clear guidelines for use of company software. In addition, IT professionals within the organization can structure information systems and establish corporate firewalls to support appropriate use of IT resources.

Self-Assessment Questions

1. A professional is someone who:
   a. requires advanced training and experience
   b. must exercise discretion and judgment in the course of his or her work
   c. does work that cannot be standardized
   d. all of the above

2. Many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional. True or False?

3. According to a study conducted by IDC, what percentage of the world's software was illegally copied (pirated) in 2004?
   a. 10–20 percent
   b. 20–30 percent
   c. 30–40 percent
   d. more than 40 percent

4. A _____ is information used in a business, generally unknown to the public, that the company has taken strong measures to keep confidential. It represents something that has economic value, has required effort or cost to develop, and has some degree of uniqueness or novelty.
   a. copyright
   b. trademark
   c. trade secret
   d. patent

5. Whistle-blowing is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. True or False?

6. Résumé inflation is a usual and customary practice tolerated by employers. True or False?

7. Society expects professionals to act in a way that:
   a. causes no harm to society
   b. provides significant benefits
   c. establishes and maintains professional standards that protect the public
   d. all of the above
8. Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean that it is ethical. True or False?
9. _____ is a process that one undertakes voluntarily to prove competency in a set of skills.
   a. Licensing
   b. Certification
   c. Registering
   d. all of the above
10. There are many international and national licensing programs for IT professionals. True or False?
11. A policy on the use of information technology can:
   a. set forth the general rights and responsibilities common to all users of information technology
   b. establish the boundaries of acceptable and unacceptable behavior
   c. enable management to take action against those who violate the policy
   d. all of the above
12. A device that serves as a barrier between a company and the outside world and limits access to the company's computer network based on the organization's Internet usage policy is a(n):
   a. Internet service provider
   b. firewall
   c. encryption device
   d. malware

Review Questions

1. What criteria would you use to define a person employed in a professional capacity? How would you define the term *IT professional*?
2. What are the six relationships in which an IT professional becomes involved? Identify at least one key issue for each of these relationships.
3. What is software piracy? What role does the Business Software Alliance take in combating software piracy?
4. How do you define a trade secret? What actions might an organization take to protect its trade secrets?
5. Identify three ethical issues that can arise in the relationship between an IT professional and a client.
6. What is a professional code of ethics? How is it different from the corporate code of conduct discussed in Chapter 1?
7. List three benefits associated with adherence to a code of professional ethics.
8. Identify four prominent IT-related professional organizations. What are some benefits of membership in each of these organizations?
9. What is the difference between vendor and industry association certification?
10. Identify three benefits of government licensing for IT professionals.
11. Identify and discuss four issues associated with the government licensing of IT professionals.
12. What is negligence? What must a plaintiff show to prove negligence?
13. What are some common ethical issues encountered by IT users? What negative impact does unethical behavior have in each of these areas?
14. What are four actions that can strengthen the ethical practices of IT users?

Discussion Questions

1. How do you prove that fraud has been committed? How do you prove breach of contract? What is the difference between the two?
2. Discuss the following topic: Laws do not provide a complete guide to ethical behavior. An activity can be legal but not ethical.
3. What is professional malpractice? Should a software engineer ever be sued for professional malpractice? Why or why not?
4. Review the ACM code of ethics in Appendix B. The code covers many of the issues an IT professional is likely to face, but not all. Identify two key issues not addressed by the ACM code of ethics.
5. What can IT professionals do to ensure that the projects they lead meet the client's expectations and do not lead to charges of fraud, fraudulent misrepresentation, and breach of contract?
6. Should all IT professionals either be licensed or certified? Why or why not?
7. What commonalities do you find among the IT professional codes of ethics discussed in this chapter? What differences are there? Are any issues that are important to you not addressed by these codes of ethics?

What Would You Do?

1. As the vice president of marketing, you hired a software contractor to build a Web site for your home building supply firm. Unfortunately, the project did not go well. From your perspective, the contractor overcommitted and underdelivered. The initial Web site was completed three months late at a cost of $2 million over the estimated $5 million. Before your site went online, a competing manufacturer launched a Web site with unique features. You demanded that these features be added to your site. This took another four months and cost an additional $1 million. To top things off, once your Web site went online, it was slow

and buggy and got hacked by a former employee of the software contractor. The contractor has estimated that it will cost another $2 million to fix these problems. You are considering suing the software contractor; however, you are concerned that this will cause further delays in the delivery of a workable Web site. What would you do?

2. You are in charge of awarding all PC service contracts for your employer. In recent e-mails with the company's PC service contractor, you casually exchanged ideas about home landscaping, your favorite pastime. You also said you would like to have a few Bradford pear trees in your yard. Upon returning from a vacation, you discover three mature trees in your yard, along with a thank-you note in your mailbox from the PC service contractor. You really want the trees, but you didn't mean for the contractor to buy them for you. You suspect that the contractor interpreted your e-mail comment as a hint that you wanted him to buy the trees. You also worry that the contractor still has the e-mail. If the contractor sent your boss a copy, it might look as if you were trying to solicit a bribe. Can the trees be considered a bribe? What would you do?
3. In Italy, *raccomandazione* is the custom of seeking and receiving special treatment from people in power or from people who are close to power. The ability to solicit favors from someone in a higher place, be it through the chief of police or the chief's chauffeur, has been part of the Italian art of getting things done for more than 2000 years. In April 2001, Italy's highest court of appeal ruled that influence peddling is not a crime. The judges did rule, however, that it is a crime to overstate one's power to exert influence.

   Your firm is opening a new sales office in Rome and will be using a local employment agency to identify and screen candidates, who will then undergo employment testing and interviews by members of your organization. What guidelines would you provide to the agency regarding the practice of raccomandazione to ensure that the agency operates ethically and effectively?
4. Jacob is the vice president of sales and an important ally of your IT department. He's gone to bat for you before the CEO on important IT projects, such as the customer relationship management system, and has valuably assisted in advocating for the use of the latest software packages within the sales organization. Jacob has played a major role in your success so far. However, you've just learned that Jacob and his support staff are using an unlicensed Lotus software suite on their desktops, while the rest of the company is standardized using Microsoft Office. You've talked to him and the rest of the company's leadership team about the need for standardized software and the risks the company runs if it uses unlicensed software, but no action has been taken. What would you do?
5. You are the new CIO at a small manufacturing company with a total of 500 employees at one plant, two warehouses, and a headquarters building. Your manager is the chief financial officer (CFO), who wants you to make it a high priority to establish a set of policies and guidelines on the use of IT resources—the firm currently has none. How would you proceed?

Cases

1. When Certification Is Justified

On June 13, 2005, Don Tennant, editor-in-chief of *Computerworld*, published an editorial in favor of IT certification and was promptly hit with a barrage of angry responses from IT professionals. They argued that testable IT knowledge does not necessarily translate into quality IT work. A professional needs good communication and problem-solving skills as well as perseverance to get the job done well. Respondents explained that hard-working IT professionals focus on skills and knowledge that are related to their current projects and don't have time for certifications that will quickly become obsolete. They suspected vendors of offering certification as a marketing ploy and a source of revenue. They accused managers without technical backgrounds of using certification as "a crutch, a poor but politically defensible substitute for knowing what and how well one's subordinates are doing."

Any manager would certainly do well to review these insightful points, yet they beg the question: what useful purposes *can* certification serve within an organization?

Robert Tekiela, vice president of technology at Sapient Corporation, asserts that many employers use certification as a means of training employees and increasing skill levels within the company. Some companies are even using certification as a perk to attract and keep good employees. American Century Investments is taking this a step further by offering a job-rotation program through which workers can acquire experience as well.

Employers are also making good use of certification as a hiring gate both for entry-level positions and for jobs that require specific core knowledge. For example, a company with a Windows Server 2003 network might run an ad for a systems integration engineer and require a Microsoft Systems Engineer (MCSE) certification. A company that uses Siebel customer relationship management software may require a new hire to have a certification in the latest version of Siebel.

In addition, specific IT fields such as project management and security have a greater need for certification. As the speed and complexity of production increase within the global marketplace, people from all industries are showing an increasing interest in project management certification. With mottos like "Do It, Do It Right, Do It Right Now," the Project Management Institute has already certified more than 100,000 people. As the IT industry recovers from declines in IT spending that followed the 2000 recession, industry employers are beginning to encourage and sometimes require project management certification.

Calls for training in the field of security management go beyond certification. The demand for security professionals is expected to double in the next three years in the face of growing threats. Spam, computer viruses, spyware, and identity theft have businesses and government organizations worried. They want to make sure that their security managers can protect their data, systems, and resources.

The best recognized security certification is the CISSP, awarded by the International Information Systems Security Certification Consortium (ISC2). Yet the CISSP examination, like so many other IT certification examinations, is multiple choice. Employers and IT professionals alike have begun to recognize the limitations of these types of examinations. They want to ensure that examinees not only have core knowledge, but know how to use that knowledge—and a multiple-choice exam, even a six-hour, 250-question exam like CISSP, can't provide this assurance.

As a result, security professionals in the UK have formed the Information Security Professionals Working Group with the purpose of raising security training to the level of other professional training. They plan to accredit academic and professional development courses and to set up a mentoring program. ISC2 also plans to run master courses and mentoring programs.

In the meantime, other organizations are catching on. Sun Computers requires the completion of programming or design assignments for some of its certifications. So, while there is no universal need for certification or a uniform examination procedure that answers all needs within the IT profession, certifying bodies are beginning to adapt their programs to better fulfill the evolving needs for certification in IT.

Questions:

1. How are Sun Computers and other vendors discussed in the chapter changing their certification programs to test for skills as well as core knowledge?
2. What are the central arguments against certification, and how can certifying bodies change their programs to overcome their shortcomings?
3. What are the benefits of certification? How can certification programs change in the future to better serve the needs of the IT community?

2. Antibribery Laws Force U.S. Companies to Raise the Bar on Business Ethics

In the mid-1970s, investigations by the U.S. Securities and Exchange Commission (SEC) revealed that more than 400 companies in the United States had made illegal or questionable payments to foreign sources. To clean up the United States' image overseas, Congress enacted the Foreign Corrupt Practices Act (FCPA), which allows the U.S. Department of Justice (DOJ) and the SEC to prosecute businesses and company personnel who bribe governments, politicians, or political parties abroad. Companies can be fined up to $2 million and be barred from doing business with the U.S. government, receiving an export license, and engaging in the securities business. People can be imprisoned for up to five years and fined twice the amount they hoped to receive as a result of the bribery.

So, executives of a large IT company today wouldn't dare bribe foreign officials, say, to obtain a large government contract. Or would they?

In the wake of the Enron scandal, a Saudi Arabian telecommunications company called National Group for Communications and Computers filed a lawsuit in a New York District Court against Lucent Technologies, claiming that the telecommunications giant, along with the Swiss company ACEC, had bribed a former Saudi Arabian minister. The telecommunications minister, Ali Al-Johani, allegedly persuaded a government-controlled company to purchase Lucent and ACEC equipment. In return, company officials purportedly gave cash gifts, paid medical and hotel bills, and made available private jets to Al-Johani between 1995 and 2002. The suit claims that these favors are worth approximately $15 million.

An amended complaint later named former Lucent CEO Richard McGinn and former chief protocol officer, Robert W. Frye, as having approved two checks totaling more than $2 million to a Seattle cancer center where Al-Johani was being treated. The complaint also fingered the CEO of Lucent's spin-off company Avaya, Donald Peterson, claiming that he signed the checks to the cancer center.

In response to these accusations against its former highest-ranking officials, Lucent launched an internal audit in 23 of its overseas operations and reported potential FCPA violations to the DOJ and the SEC. In April 2004, Lucent made headlines again when it dismissed four top Chinese officials, including President Jason Chi and Chief Operating Officer Michael Kwan. Kwan spoke out to the press, denying wrongdoing and accusing Lucent of damaging his reputation. The Chinese government subsequently failed to prosecute the executives.

In China, where certain types of bribery are pervasive, this outcome is not surprising, and the question arises: is the FCPA damaging the competitiveness of U.S. companies abroad by preventing them from securing awards that foreign companies can acquire without fear of repercussion? Congress certainly thought so in 1988, when it requested that the executive branch take measures to ensure that the United States' major trading partners adopt antibribery laws similar to the FCPA.

The FCPA further provides for affirmative defenses, the assertion that a payment considered unlawful in the United States is in fact legal in the country where it occurred. Although the Department of Justice warns that lawfulness of a payment may be difficult to prove, some acts that the FCPA would consider unlawful are perfectly legal in China. For example, if an executive pays a Chinese government official $1000 to facilitate approval procedures, the executive has acted legally according to Chinese law. To constitute criminal bribery, the value of the bribe would have to surpass a threshold of $1208. Commercial bribes under this threshold value are permitted as long as their purpose is not linked to the sale of goods or services.

Questions:

1. Lucent purportedly gave cash payments, paid medical and hotel bills, and made available private jets to Al-Johani. Under what circumstances would these actions be considered gifts? Under what circumstances would these actions be considered bribes?
2. The SEC is considering taking civil action against Lucent's former CEO Richard McGinn and Lucent's former head of Saudi Arabia operations, John Heindel. What would they have to prove to make an affirmative defense of their actions?
3. In 2004, IBM dismissed several senior executives in Korea after they were indicted by the Seoul District Prosecutor's Office, which charged that the executives used a $2.5 million slush fund to obtain contracts worth $55 million. Compare this case to Lucent's situation in China.

3. IT Usage Policy

Read the following policy on the use of IT technology for the University of Cincinnati, and use the manager's checklist in Table 2-4 to answer the following questions:

Questions:

1. Are all of the key issues covered by this policy? If not, which ones need to be addressed?
2. Is the statement of enforcement clear and strong? If not, how would you reword this section of the policy?
3. How would you ensure that this policy is communicated and understood by the broad group of IT users at the university—students, professors, research people, administrative support staff, contractors, and part-time workers?
4. Examine the IT usage policy in effect at your school. Write a paragraph identifying its strengths and weaknesses.

General Policy on the Use of Information Technology for the University of Cincinnati

As an institution of higher learning, the University both uses information technology and supplies it to the members of the University community. This policy sets forth the general rights and responsibilities common to all uses of information technology, from the simple stand-alone PC to the complex systems that create virtual classrooms, workplaces, and recreational facilities in the University.

This policy applies to all members of the University community, including guests who have been given accounts on the University's information technology systems for specific purposes. It also applies whether access is from the physical campus or from remote locations. In addition, there may be specific policies issued for individual systems, departments, colleges, and the like. While these policies must be consistent with this general policy, they provide more detailed guidance about what is allowed and what is prohibited on each system. All members of the University community are responsible for familiarizing themselves with any applicable policy prior to use.

Guiding Principles

The primary guiding principle is that the rules are the same for information technology as for other aspects of University life. The rights and responsibilities governing the behavior of members of the University community are the same on both the virtual and physical campuses, and the same disciplinary procedures will be followed when the rules are violated. There is nothing special about the virtual campus that makes it distinctly different.

The University has a strong commitment to the principles of free speech, open access to knowledge, and respect for a diversity of opinions. The rights as well as the restrictions governing these principles on the physical campus apply fully to the virtual campus.

Specific Areas

1. Applicable Laws and Regulations

   All members of the University community must obey:

   - All relevant federal, state, and local laws. These include laws of general application such as libel, copyright, trademark, privacy, obscenity, and child pornography laws, as well as laws that are specific to computers and communication systems, such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act.
   - All relevant University rules and regulations. These include the Rules of the University, the Student Code of Conduct, the various collective bargaining agreements between the University and its employees, and all other University policies, including the policy against sexual and racial harassment.
   - All contracts and licenses applicable to the resources made available to users of information technology.
   - This policy as well as other policies issued for specific systems.

2. Resource Limits

   Information technology resources are often limited; what is used by one person is no longer available to others. Many systems have specific limits on several kinds of resources, such as storage space or connect time. All users must comply with these limits and not attempt to circumvent them. Moreover, users are expected not to be wasteful of resources, whether or not there are specific limits placed on them. Unreasonable use of resources may be curtailed.

3. Privacy

   Members of the University community shall not attempt to access the private files of others. The ability to access a file does not, by itself, constitute authorization to do so.

   The University does not routinely monitor or inspect individual accounts, files, or communications. There are situations, however, in which the University has a legitimate need to do so: (1) system managers may access user accounts, files, or communications when there is reason to believe that the user is interfering with the performance of a system; (2) authorized investigators may access accounts, files, or communications to obtain relevant information when there is a reasonable suspicion that the user has violated either law or University policies; (3) coworkers and supervisors may need to access accounts, files, or communications used for University business when an employee becomes unavailable; and (4) when required by law. All monitoring and inspection shall be subject to authorization, notification, and other requirements specified in the IT Management Policy.

   Though the University will attempt to prevent unauthorized access to private files, it cannot make any guarantees. Because the University is a public entity, information in an electronic form may be subject to disclosure under the Ohio Public Records Act just as paper records are. Information also can be revealed by malfunctions of computer systems, by malicious actions of hackers, and by deliberate publication by individuals with legitimate access to the information. Users are urged to use caution in the storage of any sensitive information.

4. Access

   Some portions of the virtual campus, such as public Web pages, are open to everyone. Other portions are restricted in access to specific groups of people. No one is permitted to enter restricted areas without authorization or to allow others to access areas for which they are not authorized. The ability to access a restricted area does not, by itself, constitute authorization to do so.

   Individual accounts are for the use of the individual only; no one may share individual accounts with anyone else, including members of the account holder's family. Joint access to resources when needed should be provided from separate accounts.

5. Security

   All members of the University community must assist in maintaining the security of information technology resources. This includes physical security, protecting information, and preventing and detecting security breaches. Passwords are the keys to the virtual campus and all users are responsible for the security of their passwords. Users must report all attempts to breach the security of computer systems or networks to an appropriate official.

6. Plagiarism and Copyright

   Intellectual honesty is of vital importance in an academic community. You must not represent the work of others as your own. You must respect the intellectual rights of others and

not violate their copyright or trademark rights. It is especially important that you obey the restrictions on using software or library resources for which the University has obtained restricted licenses to make them available to members of the University community.

7. Enforcement

Anyone who becomes aware of a possible violation of this policy or the more specific regulations of the systems that comprise the virtual campus should notify the relevant department head or system administrator. The administrator will investigate the incident and determine whether further action is warranted. The administrator may resolve minor issues by obtaining the agreement that the inappropriate action will not be repeated. In those cases that warrant disciplinary action, the system administrator will refer the matter to the appropriate authorities. These include Public Safety for violations of criminal law, the Office of Student Affairs for violations by students, the appropriate Provost for violations by faculty, and the Office of Human Resources for violations by staff members.

System administrators can act to block access and disable accounts when necessary to protect the system or prevent prohibited activities, but such actions cannot be used as punishments. Users must be notified promptly of the action and the restrictions must be removed unless the case is referred for disciplinary action.

End Notes

[1] "Settlement Reached Over PeopleSoft Implementation," *On Campus*, www.csuohio.edu/oncampus/2005/0307e.html, March 07, 2005.

[2] Olsen, Florence, "Delays, Bugs, and Cost Overruns Plague PeopleSoft's Services," *The Chronicle of Higher Education*, http://chronicle.com/free/v46/i05/05a03101.htm, September 24, 1999.

[3] Olsen, Florence, "Cleveland State U. Sues Consulting Company That Managed Its PeopleSoft Installation," *The Chronicle of Higher Education*, chronicle.com/free/2002/05/2002051302t.htm, May 13, 2002.

[4] Songini, Marc L., "University Pins $510M Lawsuit on PeopleSoft," *Computerworld*, www.computerworld.com/softwaretopics/erp/story/0,10801,91720,00.html, March 29, 2004.

[5] Stedman, Craig, "ERP Problems Plague College," *Computerworld*, www.computerworld.com/news/1999/story/0,11280,37669,00.html, November 22, 1999.

[6] Wailgum, Thomas, "Big Mess on Campus," *CIO*, www.cio.com/archive/050105/college.html, May 1, 2005.

[7] Business Software Alliance, "2nd Annual BSA and IDC Global Software Piracy Study," www.bsa.org/globalstudy/, July 8, 2005.

[8] "Business Software Alliance," Wikipedia, en.wikipedia.org/wiki/Business_Software_Alliance, July 8, 2005.

[9] Williams, Martyn, "Jury Awards Lexar Another $84 Million in Toshiba Case," *Computerworld*, www.computerworld.com, March 25, 2005.

[10] Evers, Jorvis, "Oracle Pays $8 Million to Settle Suit Over Training Charges," *Computerworld*, www.computerworld.com, May 16, 2005.

[11] Cheeseman, Henry R., *Contemporary Business Law*, Prentice-Hall, 2000, page 249.

[12] Cheeseman, Henry R., *Contemporary Business Law*, Prentice-Hall, 2000, page 292.

[13] Cheeseman, Henry R., *Contemporary Business Law*, Prentice-Hall, 2000, page 292.

[14] Chabrow, Eric, "See You In Court," *InformationWeek*, www.informationweek.com, July 25, 2005.

[15] Adler, Edward C., *The Complete Reference Checking Book*, AMACOM, a division of the American Management Association, 2003.

[16] AITP Web site, www.aitp.org, July 12, 2005.

[17] About the Computer Society, IEEE-CS Web site, www.computer.org/portal/site/ieeecs/, July 12, 2005.

[18] Tekiela, Robert, "How To Get Value from Technology Certifications," *Computerworld*, www.computerworld.com, December 22, 2004.

[19] Institute for Certification of Computing Professionals, www.iccp.org, July 18, 2005.

[20] "Certified Computing Professional," Institute for Certification of Computing Professionals, www.iccp.org, July 18, 2005.

[21] "Licensing Information—Who Should Be Licensed," Texas Board of Professional Engineers, www.tbpe.state.tx.us, July 25, 2005.

[22] "PE Electrical and Computer Exam," www.ncees.org/exams/professional/pe_electrical_exams.php, July 16, 2005.

[23] Martens, China, "Survey: Computer Porn Remains Issue at U.S. Corporations," *Computerworld*, www.computerworld.com, June 21, 2005.

Sources for Case 1

"About the Profession," Project Management Institute Web site, www.pmi.org/info/PP_AboutProfessionOverview.asp?nav=0501.

"Project Managers," *ComputerWeekly.com*, www.computerweekly.com/Jobs/2005/08/02/11071/Project+Managers.htm, August 09, 2005.

Goodwin, Bill, "Blueprint for Professionalism In IT Security," *ComputerWeekly.com*, www.computerweekly.com/Articles/2005/01/19/207802/BlueprintforprofessionalisminITsecurity.htm, January 19, 2005.

Hoffman, Thomas, "Demand for IT Certifications on the Rise," *Computerworld*, www.computerworld.com/careertopics/careers/story/0,10801,99903,00.html, February 21, 2005.

Nicolle, Lindsay, "Open the Door to a Secure Career," *ComputerWeekly.com*, www.computerweekly.com/Articles/2005/02/07/208200/Openthedoortoasecurecareer.htm, February 7, 2005.

Tekiela, Robert, "How to Get Value from Technology Certifications," *Computerworld*, www.computerworld.com/careertopics/careers/story/0,10801,98449,00.html, December 22, 2004.

Tennant, Don, "Certifiably Concerned," *Computerworld*, www.computerworld.com/careertopics/careers/training/story/0,10801,102394,00.html, June 13, 2005.

Tennant, Don, "Certifiably Mad?" *Computerworld*, www.computerworld.com/careertopics/careers/story/0,10801,102564,00.html, June 20, 2005.

Weiss, Todd, "Profile: American Century Investments," *Computerworld*, www.computerworld.com/careertopics/careers/story/0,10801,102712,00.html, June 27, 2005.

Sources for Case 2

"Firing of Lucent Executives Highlights Calls for Transparency in China," *China High Tech PR*, www.chinahightechpr.com/fullArticle.cfm?code=318, April 2004.

"Foreign Corrupt Practices Act Antibribery Provisions," U.S. Department of Justice Web site, www.usdoj.gov/criminal/fraud/fcpa/dojdocb.htm.

Associated Press, "Saudi Suit Claims Lucent OK'd Bribes," *The Boston Globe*, www.boston.com/business/technology/articles/2004/03/19/saudi_suit_claims_lucent_okd_bribes?mode=PF, March 19, 2004.

IDG News Service, "Lucent Fires Top Chinese Executives for Bribery," *ITWorld.com*, www.itworld.com/Man/2698/040407lucentchina/, April 7, 2004.

Leyden, John, "Saudi Firm Accuses Lucent of Bribery," *The Register*, www.theregister.co.uk/2003/08/13/saudi_firm_accuses_lucent/, August 13, 2003.

Reuters, "4 Lucent Execs to Leave After Saudi Probe," *USA Today*, www.usatoday.com/money/industries/telecom/2004-04-06-lucent_x.htm, April 6, 2004.

Reuters, "Lucent Names Shen to Head China After Ousters," *The Union Tribune*, www.signonsandiego.com/news/business/20040913-0251-telecoms-lucent-shen.html, September 13, 2004.

Tjoa, Laetitia, Jianyu, Ouyang, and Pykstra, Like, "Complying with PRC Antibribery Laws," *The China Business Review*, www.chinabusinessreview.com/public/0503/wong.html, March-April 2005.

CHAPTER 3

COMPUTER AND INTERNET CRIME

QUOTE

In view of all the deadly computer viruses that have been spreading lately, Weekend Update would like to remind you: when you link up to another computer, you're linking up to every computer that that computer has ever linked up to.
—Dennis Miller, *Saturday Night Live*, U.S. television show

VIGNETTE

Treatment of Sasser Worm Author Sends Wrong Message

Unleashed in April 2004, the Sasser worm hit IT systems around the world hard and fast. Unlike most computer viruses before it, the Sasser worm didn't spread through e-mail, but moved undetected across the Internet from computer to computer. It exploited a weakness in Microsoft Windows XP and Windows 2000 operating systems. By the first weekend in May, American Express, the Associated Press, the British Coast Guard, universities, and hospitals reported that the Sasser worm had swamped their systems. Computer troubles led Delta Airlines to cancel 40 flights and delay many others.

Microsoft quickly posted a $250,000 reward, and by mid-May, authorities apprehended Sven Jaschen, a German teenager. Jaschen confessed and was convicted after a three-day trial. Jaschen could have received up to five years in prison, but because he was tried as a minor, the court suspended his 21-month sentence, leaving him with only 30 hours of community service.