CHAPTER 2

ETHICS FOR IT WORKERS AND IT USERS

QUOTE

Always do right—this will gratify some and astonish the rest.
—Mark Twain

marekuliasz/Shutterstock.com

ORGANIZATIONS BEHAVING BADLY

Queensland, the second largest state in Australia, awarded an outsourcing contract to IBM to build a new payroll application for its Department of Health at an initial cost estimate of $5 million. The project, however, went horribly wrong. Among other issues, the resulting system, delivered many months late, generated incorrect checks for some staff and no checks at all for others. As efforts mounted to fix the problems, the project cost ballooned out of control, eventually reaching more than $1 billion.

Subsequent investigation by the state led to the allegations that IBM employees had acted unethically during the bidding process. In a report issued after the investigation, the Queensland government asserted that it would not have contracted with IBM were it not for misrepresentations made by IBM regarding its expertise as well as the true project costs. For its part, IBM claimed that Queensland employees did a terrible job in managing the project—a claim supported by the state's own investigation.[1,2]

Successful IT outsourcing projects require the development of strong working relationships among members of the client organization and the outside organization that are built on a solid foundation of trust. Unfortunately, many attempts at outsourcing fail—often due to poor working relationships, as this example shows. What are the keys to developing successful working relationships? Who bears responsibility for forming such relationships—the client or the service provider?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What relationships must an IT worker manage, and what key ethical issues can arise in each?
2. What can be done to encourage the professionalism of IT workers?
3. What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

IT WORKER RELATIONSHIPS THAT MUST BE MANAGED

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

Relationships Between IT Workers and Employers

IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT worker and an employer typically agree on the fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance

expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits. Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. Topics addressed in such a manual or code of conduct might include protection of company secrets; vacation policy; time off allowed for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.

Other aspects of this relationship develop over time, depending on circumstances (for example, whether the employee can leave early one day if the time is made up 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 issues are specific to the role of the IT worker 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 workers must set an example and enforce policies regarding the ethical use of IT. IT workers often have the skills and knowledge to abuse systems and data or to enable others to do so. Software piracy is an area in which IT workers may be tempted to violate laws and policies. Although end users often 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 members—either they allow it to happen or they actively engage in it, often to reduce IT-related spending.

The **Software & Information Industry Association (SIIA)** and the **BSA | The Software Alliance (BSA)** are trade groups that represent the world's largest software and hardware manufacturers. Part of their mission is to stop the unauthorized copying of software produced by its members. North America has the lowest regional rate of software piracy at 17 percent, which represents a commercial value of $10 billion in lost revenue for software development companies.[3] The global software theft rate for personal computer software is around 43 percent, which equates to a commercial value of $62.7 billion.[4]

SIIA promotes the common interests of the software and digital content industry. It protects the intellectual property of member companies and advocates a legal and regulatory environment that benefits the entire industry. SIIA informs the industry and the broader public by serving as a resource on trends, technologies, policies, and related issues that affect member firms and demonstrate the contribution of the industry to the broader economy. It also provides global services in government relations, business development, corporate education, and intellectual property protection. Over 200 organizations are members of SIIA, including 21st Century Fox, Accenture, Adobe Systems, Bank of America Merrill Lynch, Blackboard, Cengage Learning, Fidelity Investments, Google, Scottrade, Thomson Reuters, and Wells Fargo Bank.[5]

BSA is funded both through dues based on member companies' software revenue and through settlements from companies that commit piracy. BSA membership includes about two dozen global members such as Adobe, Apple, Dell, IBM, Intuit, Microsoft, Oracle, and SAS Institute. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA website (*www.nopiracy.org*), and

referrals from member companies. Many of these cases are reported by disgruntled employees or former employees who can receive a monetary reward of thousands of dollars. In 2012 alone, BSA investigated over 15,000 reports of unlicensed software use around the globe.[6]

When the BSA receives what it believes to be a credible tip, it contacts the company and informs it that a tip has been received. It then requests a detailed inventory of all software used by the company, plus evidence of the appropriate licenses for each piece of software. Should the company have insufficient licenses, it has two choices: purchase the required number of licenses and pay BSA a fine, or stonewall and risk the BSA working with the U.S. Marshall's office to obtain a search warrant to search its premises. Strong probable cause evidence is required to obtain the search warrant, but it has been done in the past resulting in expensive and time-consuming litigation, as well as significant business interruption.

Shortly after its one IT staff member left the company, a Texas automotive repair company received a letter from the BSA accusing it of using unlicensed copies of Microsoft software. The company was threatened with a multimillion-dollar fine, one it could not pay and that would force it out of business. To stave off bankruptcy, the company froze salaries and put off the purchase of needed equipment. The dispute was eventually settled for a fraction of the initial amount after the company sought out legal counsel.[7]

Trade secrecy is another area that can present challenges for IT workers and their employers. A **trade secret** is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty. Trade secrets can include the design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes. Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke, and Intel's manufacturing process for the Core i7-6950K 10-core processing chip. Employers worry that employees may reveal these secrets to competitors, especially if they leave the company. As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Zillow is an online real estate and rental marketplace that provides information for people interested in buying, selling, renting, financing, and remodeling homes and apartments. Through the company's website and app, users can access a database of more than 110 million U.S. homes—including homes for sale, homes for rent, and even homes not currently on the market. Zillow also provides a range of services, including one it calls Zestimate, which provides an estimated market value for a house, and a similar service call Rent Zestimate, which estimates the current market rate for rent for a particular property. Move is a rival company offering similar services. In early 2014, Move's chief strategy officer resigned and, on the same day, joined Zillow as its second highest paid executive. Move filed suit against Zillow, alleging that its former employee, and by extension Zillow, stole trade secrets and proprietary information by copying thousands of document and deleting texts and emails from his company-issued computer and smartphone before resigning.[8] Further, Move alleged that Zillow attempted to cover up the theft. Following more than two

years of legal wrangling, Zillow agreed to pay Move a total of $130 million to settle the allegations, with the stipulation that Zillow is not admitting liability in the settlement.[9]

Another issue that can create friction between employers and IT workers 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 computer 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 might 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, perhaps resulting in retaliation and firing.

Amazon, IBM, Microsoft, Oracle, and SAP, along with many other companies, are competing in the rapidly growing cloud services arena. Competition is fierce, and the companies all have an incentive to make their cloud services appear financially successful. However, a whistle-blower lawsuit recently filed against Oracle highlighted potential issues related to the way such companies account for income from subscription-based software services that run in the cloud. The whistle-blower, a former Oracle employee, accused management of pressuring her to add millions of dollars in accruals to financial reports for expected cloud-based software and services revenue. Accounting experts acknowledge that classifying software sales as cloud or traditional is complex and requires determinations that might subsequently be challenged by auditors. Nonetheless, Oracle shares dropped 4 percent the day following announcement of the lawsuit.[10] Although Oracle alleges the whistle-blower was fired for poor performance, the employee maintains that she was let go just two months after she received a positive job performance review and just one month after the alleged incident began. Oracle strongly denies any allegations of wrongdoing and has vowed to countersue the whistle-blower for malicious prosecution.[11]

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same company as the IT worker. In other cases, the client is part of a different company. In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame. For example, an IT worker might agree to implement a new accounts payable software package that meets a client's requirements. The client provides compensation, access to key contacts, and perhaps a 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 technical expertise

between IT workers 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 the IT worker. The client trusts the IT worker to use his or her expertise and to act in the client's best interests. The IT worker must trust that the client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand the impact of key decisions, and use the information to make wise choices among various alternatives. Thus, the responsibility for decision making is shared between the client and the IT worker.

One potential ethical problem that can interfere with the relationship between IT workers and their 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. Such a situation has the potential to undermine the objectivity of an IT worker due to a **conflict of interest**—a conflict between the IT worker's (or the IT firm's) self-interest and the client's interests. 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 would raise questions about the vendor's objectivity and the trustworthiness of its recommendations.

Problems can also arise during a project if IT workers find themselves unable to provide full and accurate reporting of the project's status due to a lack of information, tools, or experience needed 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 such a situation, the client may not be informed about a 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 described next.

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 a misrepresentation. To prove fraud in a court of law, prosecutors must demonstrate the following elements:

- The wrongdoer made a false representation of material fact.
- The wrongdoer intended to deceive the innocent party.
- The innocent party justifiably relied on the misrepresentation.
- The innocent party was injured.

Misrepresentation is the misstatement or incomplete statement of a material fact. If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.

Affinity Gaming, a Las Vegas-based casino with 11 properties located across four states, suffered a data breach in 2013 that enabled hackers to gain access to customers' credit card data. Affinity hired Trustwave, an information security company that provides on-demand threat, vulnerability, and compliance-management services to investigate and contain the breach. Following its investigation, Trustwave claimed that it had identified how the data breach had occurred and had contained the malware responsible for it. However, a year later, Affinity was hit with a second customer data breach. This time, Affinity hired Mandiant, a Trustwave competitor, to conduct an investigation. Mandiant concluded that Trustwave's original work was incomplete and had failed to identify the means by which the attacker had breached Affinity's data security. Affinity sued Trustwave for conducting an allegedly "woefully inadequate" investigation that missed key details of the network breach and enabled subsequent attacks. Affinity alleged that Trustwave made misrepresentations when it claimed that its examination would analyze and help remedy the data breach, when it represented that the data breach was "contained," and when it claimed that its recommendations would address the data breach.[12]

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, which impairs or destroys 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. "When there has been a material breach of contract, the non-breaching 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]

In 2016, Hewlett-Packard Enterprise (HPE) was awarded $3 billion in damages from Oracle after a court determined that Oracle had breached its contract with HPE by dropping support for all Oracle database software being run on HP systems using Intel's Itanium processor chip. HPE argued that Oracle's actions dramatically reduced the sale of HPE's Itanium-based products. HPE also alleged that Oracle's actions were intended to boost sales of Oracle's own Sun hardware. The jury ultimately agreed with HPE and awarded it the full amount it was seeking, compensating the company for both lost sales and damages, as well as requiring Oracle to continue supporting Itanium-based systems.[14]

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, the vast majority 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. Clients and vendors often disagree about who is to blame in such circumstances. Frequent causes of problems in IT projects include the following (see Figure 2-1):

- Scope creep—Changes to the scope of the project or the system requirements can result in cost overruns, missed deadlines, and a project that fails to meet end-user expectations.
- Poor communication—Miscommunication or a lack of communication between customer and vendor can lead to a system whose performance does not meet expectations.
- Delivery of an obsolete solution—The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- Legacy systems—If a customer fails to reveal information about legacy systems or databases that must connect with the new hardware or software at the start of a project, implementation can become extremely difficult.

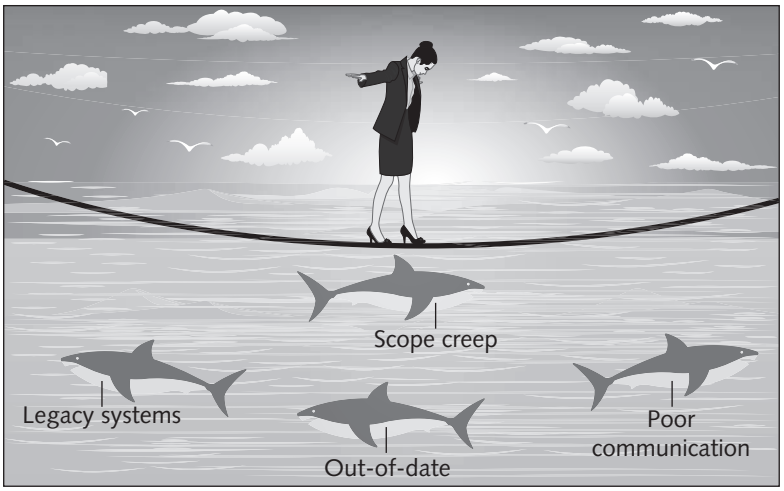

FIGURE 2-1 Frequent causes of problems in IT projects

Relationships Between IT Workers and Suppliers

IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as 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 worker may never have considered.

IT workers can 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 build a good working relationship.

Suppliers strive to maintain positive relationships with their customers in order to make and increase sales. To achieve this goal, they may sometimes engage in unethical actions—for example, offering an IT worker a gift that is actually intended as a bribe. Clearly, IT workers should not accept a bribe from a vendor, and they must be careful when 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 it may be perceived as bribery by an auditor.

Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage. An obvious example is a software supplier sales representative who offers money to another company's employee to get its business. This type of bribe is often referred to as a kickback or a payoff. The person who offers a bribe commits a crime when the offer is made, and the recipient is guilty of a crime if he or she accepts the bribe. Various states have enacted bribery laws, which have sometimes been used to invalidate contracts involving bribes but have seldom been used to make criminal convictions.

Foxconn Technology, the world's largest electronics contract manufacturer, is headquartered in New Taipei City, Taiwan. The company assembles products for top international brands such as Apple, Nokia, and Sony, and it procures supplies for those products from a wide range of suppliers. In 2014, five former Foxconn employees, including two former senior managers, were charged with bribery for accepting kickbacks from 10 suppliers in exchange for purchasing contracts and assistance clearing Foxconn's quality control checks. Foxconn officials detected the problem and alerted authorities in both Taiwan and China following an internal audit.[15]

Internal control is the process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. An organization's internal control resources include all the people, policies, processes, procedures, and systems controlled by management that enable it to meet these goals (see Figure 2-2).

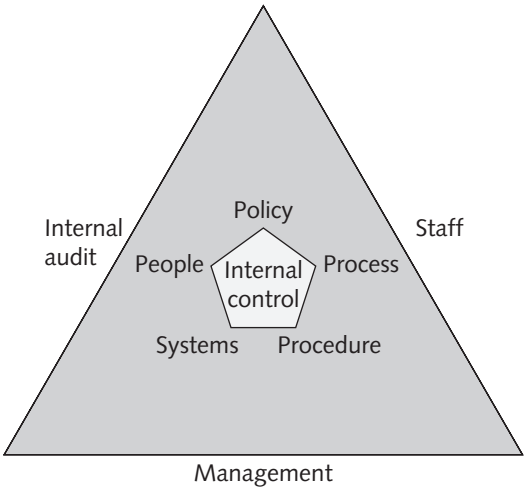

FIGURE 2-2 Internal control

Policies are the guidelines and standards by which the organization must abide. The guidelines and standards are often in response to some law. Policies drive processes and procedures. **Processes** are a collection of tasks designed to accomplish a stated objective. A **procedure** defines the exact instructions for completing each task in a process. An organization might have a policy that defines the credit terms and collection guidelines to be followed when handling a customer order. The processes associated with handling customer orders could include creating a new customer account, accepting a new order from an existing customer, and planning shipment of a customer order, among others. Procedures for each process define how to complete each task in the process. The process and procedures must be designed and executed to conform to the credit terms and collection guidelines policy.

Management is responsible for ensuring that an adequate system of internal control is set up, documented with written procedures, and implemented. Management must also decide the proper level of control over various aspects of the business so that the cost of implementing control does not outweigh the benefits. Employees are responsible for following the documented procedures and reporting to management if the controls are not effective in meeting the needs of the organization. The internal audit organization is responsible for assessing whether the internal controls have been implemented correctly and are functioning as designed; the internal audit organization reports its findings to management.

A fundamental concept of good internal controls is the careful **separation of duties** associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people. With proper separation of duties, fraud would require the collusion of two or more parties. When designing an accounts receivable system, for instance, the principal of separation of duties dictates that you separate responsibility for the receipt of customer payments, approving write-offs, depositing cash, and reconciling bank statements. Ideally, no one person should be allowed to perform more than one of these tasks. Internal controls play a key role in preventing and detecting fraud and protecting the organization's resources. Proper separation of duties is frequently reviewed during the audit of a business operation.

In small organizations, it is common for employees to have multiple responsibilities. Separation of duties is often not practical, and internal controls are more likely to be informal and carried out by one or a few people. Such a lack of separation of duties raises concerns that fraud could go undetected. Monitoring and reviewing cash receipt and disbursement activities by supervisory personnel not directly involved with the daily processing is one way to improve internal control within a small organization.

The **Foreign Corrupt Practices Act (FCPA,** 15 U.S. Code § 78dd-1) 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 and 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 5 years.

Importantly, the FCPA also requires corporations whose securities are listed in the United States to meet U.S. accounting standards by having an adequate system of internal control, including maintaining books and records that accurately and fairly reflect all transactions—the so-called books and records provision of the act. 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 must be audited by both internal and outside auditors to ensure that they meet these standards. Thus, it is not enough for an organization to simply direct its employees or agents to not accept or offer bribes; rather, it must also keep a set of books and establish a system of internal control to prevent bribery from occurring.

Hewlett-Packard (HP) agreed to pay $108 million to resolve FCPA-related investigations by the U.S. Department of Justice and the Securities and Exchange Commission into whether HP subsidiaries in Mexico, Poland, and Russia bribed government officials to obtain highly profitable contracts. The investigation revealed that HP's "subsidiaries created a slush fund for bribe payments, employed two sets of books to track bribe recipients, and used anonymous email accounts and prepaid mobile telephones to arrange covert meetings to hand over bags of cash," according to Deputy Assistant Attorney General Bruce Swartz. In a statement issued when the settlement was announced, HP executive vice president and general counsel John Schultz said HP fully cooperated with the investigation and that the misconduct was limited to a small number of people who were no longer employed by the company.[16]

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. But, at what point does a gift become a bribe, and 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 that all gifts be declared and that everything but token gifts be declined. Some companies have a policy of pooling the gifts received by their employees, auctioning them off, and giving the proceeds to charity.

When it comes to distinguishing between bribes and gifts, the perceptions of the donor and the 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 2-1 shows the key distinctions between bribes and gifts.

TABLE 2-1 Distinguishing between bribes and gifts

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 Workers and Other Professionals

Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often 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 viewed 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 among members of the IT profession. One of the most common is **résumé inflation**, which involves lying on a résumé by, for example, claiming competence in an IT skill that is in high demand. Even though an IT worker might benefit in the short term from exaggerating his or her qualifications, such an action can hurt the profession and the individual in the long run. Many employers consider lying on a résumé as grounds for immediate dismissal. For instance, Yahoo hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012; however, Thompson resigned less than a year later over discrepancies in his academic record summarized on his résumé.[17] Some studies have shown that around 30 percent of all U.S. job applicants exaggerate their accomplishments, while roughly 10 percent "seriously misrepresent" their backgrounds.[18] Table 2-2 lists the areas of a résumé that are most prone to exaggeration.

TABLE 2-2 Most frequent areas of résumé falsehood or exaggeration

Area of exaggeration	Frequency (%)	How to uncover the truth
Embellished skill set	57	Verification of licenses and/or certifications with accrediting agency
Embellished responsibilities	55	Thorough background and reference checks
Dates of employment	42	Thorough background and reference check
Job title	34	Thorough background and reference check
Academic degrees earned	33	Verification of education claims with educational institutions
Companies worked for	26	Thorough background and reference check
Accolades/Awards	18	Thorough background and background check

Source: "Infographic: The Lies We Tell on Resumes," Background Checks.org, http://backgroundchecks.org/infographic-the-lies-we-tell-on-resumes.html.

Another ethical issue that can arise in relationships between IT workers and other professionals is the inappropriate sharing of corporate information. Because of their roles, IT workers may have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on. It might be sold to other organizations or shared informally during

work conversations with others who have no need to know. Revealing such private or confidential information is grounds for termination in many organizations and could even lead to criminal charges.

The Office of Communications (aka Ofcom) is the regulatory and competition authority for the broadcasting, telecommunications, and postal industries in the United Kingdom. In 2016, Ofcom made headlines when one of its former short-term contract employees offered his new employer (UKTV, a multichannel broadcaster jointly owned by BBC Worldwide and Scripps Networks Interactive), six years of confidential income and spending data of competing broadcasters that had been submitted to Ofcom in its regulatory capacity. The data were stolen from Ofcom's market intelligence database and would have provided valuable insights into competitors' programming budgets and revenue streams. UKTV management acted quickly to fire the individual and reported the incident to Ofcom. In a letter to other broadcasters, UKTV promised that it had removed all the data from its systems, assuring its rivals that the data had not been used.[19]

Relationships Between IT Workers and IT Users

The term **IT user** refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

IT workers 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. They also have a key responsibility to establish an environment that supports ethical behaviors by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

Relationships Between IT Workers and Society

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

Clearly, the actions of an IT worker can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process. A failure or an error in the system may put workers or people who live near the plant at risk. As a result, IT workers have a relationship with members of society who may be affected by their actions. There is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public. However, as discussed in the following sections, there are a number of professional organizations that provide useful professional codes of ethics to guide actions that support the ethical behavior of IT workers.

CRITICAL THINKING EXERCISE: ACCEPT THE TICKETS OR NOT?

You are leading your organization's effort to purchase and install new accounting software. The project will cost an estimated $3 million, and over the past few months, you have had meetings with several potential vendors to evaluate their offerings and capabilities. It is early March, and the National Collegiate Athletic Association (NCAA) basketball tournament is underway. You receive a phone call from one of the sales reps you met with recently. He has two tickets to the second-round games next weekend and wants to give them to you. Can you accept this offer without raising any concerns? How can you turn down this offer without offending the sales rep? Would accepting the offer from the sales rep obligate you in any way? Would you feel compelled to share information with him about where his firm stands in the competition for your business? Would you provide him with any insights about how his firm could make its bid more attractive? Would you be more inclined to spend additional time interacting with him to better understand his firm's products and services?

ENCOURAGING THE PROFESSIONALISM OF IT WORKERS

A professional is one who possesses the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well. Organizations—including many IT organizations—are desperately seeking workers who have the following characteristics of a professional:

- They are an expert in the tools and skills needed to do their job.
- They adhere to high ethical and moral standards.
- They produce high quality results.
- They meet their commitments.
- They communicate effectively.
- They train and develop others who are less skilled or experienced.

IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available. Each of these topics is discussed in the following sections.

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 2,000-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 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.

Laws do not provide a complete guide to ethical behavior. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a definitive collection of behavioral standards. However, following a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

- *Ethical decision making*—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.
- *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 acceptable and unacceptable behaviors 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 exist in the IT arena.
- *Trust and respect from the general public*—Public trust is built on the expectation that a professional will behave ethically. People must often 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 for professionals and their profession.
- *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 one IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT workers. However, the existence of such organizations is useful in a field that is rapidly growing and changing. In order to stay on the top of the many new developments in their field, IT workers need to network with others, seek out new ideas, and continually build on their personal skills and expertise. Whether you are a freelance programmer or the CIO of a *Fortune* 500 company, membership in an organization of IT workers enables you to associate with others of similar work experience, develop working relationships, and exchange ideas. These organizations disseminate information through email, periodicals, websites, social media, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed codes of ethics. Four of the most prominent IT-related professional organizations are highlighted in the following sections.

Association for Computing Machinery (ACM)

The Association for Computing Machinery (ACM), a computing society founded in New York in 1947, is "dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests by fostering the open interchange of information and by promoting the highest professional and ethical standards."[20] ACM is the world's largest educational and scientific society and is international in scope, with ACM councils established in Europe, India, and China. Over half the organization's 100,000 student and professional members reside outside the United States in more than 100 countries. Its leading magazine, *Communications of the ACM*, provides industry news, commentary, observations, and practical research. In addition, the ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.[21] The ACM Code of Ethics can be found at *https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct#top*.

Institute of Electrical and Electronics Engineers Computer Society (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 about 60,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.[22]

Association of Information Technology Professionals (AITP)

The Association of Information Technology Professionals (AITP) started in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the IBM punched-card tabulating machines they were operating—a precursor of the modern electronic computer. They were members of a local group called the Machine Accountants Association (MAA), which first evolved into the Data Processing Management Association in 1962 and finally the AITP in 1996.[23]

The AITP provides IT-related seminars and conferences, information on IT issues, and forums for networking with other IT workers. 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 within their industry. The AITP also has a code of ethics and standards of conduct. The standards of conduct are considered to be rules that no true IT professional should violate. The AITP Code of Ethics and Standards of Conduct can be found at *https://www.aitp.org/?page=EthicsConduct*.

SysAdmin, Audit, Network, Security (SANS) Institute

The SysAdmin, Audit, Network, Security (SANS) Institute provides information security training and certification for a wide range of individuals, such as auditors, network administrators, and security managers. Each year, its programs train some 12,000 people, and a total of more than 165,000 security professionals around the world have taken one or

more of its courses. SANS publishes a semiweekly news digest (*NewsBites*), a weekly security vulnerability digest (*@Risk*), and flash security alerts.[24]

At no cost, SANS makes available a collection of some 1,200 research documents about various information security topics. SANS also operates Internet Storm Center—a program that monitors malicious Internet activity and provides a free early warning service to Internet users—and works with Internet service providers to thwart malicious attackers. The SANS Institute IT Code of Ethics can be found at *https://www.sans.org/security-resources/ethics?ref=3781*.

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 (for example, the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products) and is generally voluntary. IT-related certifications may or may not include a 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 about the value of certifications. 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 plan to help them continue to grow and advance in their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.

Deciding on the best IT certification—and even whether to seek a certification—depends on the individual's career aspirations, existing skill level, and accessibility to training (Table 2-3). Is certification relevant to your current job or the one to which

TABLE 2-3 Common IT industry certifications

Category	Certification	Certifying organization
Security	CompTIA Security+	Computer Technology Industry Association
Security	Certified Security Analyst	International Council of E-commerce Consultants (EC)
Forensics	Certified Computer Examiner	The International Society of Forensic Computer Examiners
Governance	Certified in the Governance of Enterprise IT	ISACA
Project management	Project Management Professional	Project Management Institute

you aspire? Does the company offering the certification have a good reputation? What is the current and potential future demand for skills in this area of certification?

Vendor Certifications

Many IT vendors—such as Cisco, IBM, Microsoft, SAP, and Oracle—offer certification programs for those who use 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 an IT worker's salary and career prospects. Certifications that are tied to a vendor's product are relevant for job roles with very specific requirements or certain aspects of broader roles. Sometimes, however, vendor certifications are too narrowly focused on the technical details of the vendor's technology and do not address more general concepts.

To become certified, one must pass a written exam. Because of legal concerns about whether other types of exams can be graded objectively, most exams are presented in a multiple-choice format. A few certifications, such as the Cisco Certified Internetwork Expert (CCIE) certification, 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 such support can be expensive. Depending on the certification, study materials can cost $1,000 or more, and in-class formal training courses often cost more than $10,000. Table 2-4 lists some of the common vendor certifications.

TABLE 2-4 Common vendor-specific certifications for IT workers

Category	Certification
MAC OS X	Apple Certified Technical Coordinator
Cisco Hardware	Cisco Certified Design Associate
Cisco Networking	Cisco Certified Network Professionals
Cisco Networking	Cisco Certified Internetwork Expert
Microsoft Products	Microsoft Certified Professional
Citrix Products	Citrix Certified Administrator (CCA)
Oracle Database	Oracle Database 12c: Certified Expert Performance Management and Tuning
Salesforce software	Salesforce.com Certified Administrator

Licensing of IT Professionals

In the United States, a **government license** is government-issued permission to engage in an activity or to operate a business. Most states license activities that could result in damage to public health, safety, or welfare—if practiced by an individual who has not

demonstrated minimal competence. Licensing is generally administered at the state level and often requires that the recipient pass a test of some kind. Some professionals must be licensed, including certified public accountants (CPAs), lawyers, doctors, various types of medical and daycare providers, and some engineers.

The Case for Licensing IT Workers

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another, and every day, the public entrust their health, safety, and welfare to these systems. Software systems are embedded in the vehicles we drive, controlling functions such as braking, cruise control, airbag deployment, navigation, and parking. Even more advanced systems are being designed and built for "self-driving" vehicles. Complex computers and information systems manage and control the autopilot functions of passenger planes, the nuclear reactors of power plants, and the military's missile launch and guidance systems. Complex medical information systems monitor hospital patients on critical life support. Failure of any of these systems can result in human injury or even death.

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 about whether the licensing of IT workers would improve information systems. Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice. State licensing boards have ultimate authority over the specific requirements for licensing in their jurisdiction, and also decide whether or not to even offer a given exam.

In 1993, the ACM and IEEE-CS 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 core **body of knowledge** for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. The "Software Engineering Code of Ethics and Professional Practice" documents the ethical and professional responsibilities and obligations of software engineers. (A **software engineer** is defined as one who applies engineering principles and practices to the design, development, implementation, testing, and maintenance of software.) After a thorough review process, version 5.2 of the Software Engineering Code of Ethics and Professional Practice was adopted by both the ACM and IEEE-CS (see Figure 2-3).[25] The code contains eight principles related to the behavior of and decisions made by software engineers, including practitioners, educators, managers, supervisors, and policy makers, as well as trainees and students of the profession.

The nonprofit organization National Council of Examiners for Engineering and Surveying (NCEES) develops, administers, and scores the examinations used for engineering and surveying licensure in the United States. Members of NCEES include the licensing

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. Public - Software engineers shall act consistently with the public interest.
2. Client and Employer - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. Product - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. Judgment - Software engineers shall maintain integrity and independence in their professional judgment.
5. Management - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. Profession - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. Colleagues - Software engineers shall be fair to and supportive of their colleagues.
8. Self - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

FIGURE 2-3 Software Engineering Code of Ethics and Professional Practice

Source: Software Engineering Code of Ethics and Professional Practice. © acm.org, 2015. http://www.acm.org/about/se-code

boards for all 50 states.[26] In 2013, NCEES began offering testing for software engineers. The eight-hour exam consisting of 80 multiple-choice questions was produced in collaboration with the Institute of Electrical and Electronic Engineers (IEEE).[27] As of 2015, 40 states and U.S. jurisdictions support the licensing of software engineers. The software engineering license certifies that the license holder has:

- completed an appropriate engineering education from a program accredited by the Accreditation Board for Engineering and Technology/Engineering Accreditation. (As of October 2015, there are 23 accredited software engineering programs in the United States and 239 computer engineering programs in the United States.)
- at least four years of software engineering experience in his or her field (the required years of experience varies by state) working under the supervision of qualified engineers. (This could be a sticking point because there are so few licensed software engineers.)
- passed the following two NCEES engineering exams: (1) the Fundamentals of Engineering exam, which is a broad-based exam and (2) an eight-hour software engineering Principles and Practices exam, which covers topics such as software requirements, design, construction, testing, maintenance, configuration management, engineering processes, quality assurance, safety, security, and privacy.
- kept current by meeting his or her state's minimum continuing education requirements.

For most IT workers, becoming licensed as a software engineer is optional because they practice under the "industrial exemption" clause of their state's licensing laws that permits them to work internally for an organization without licensure so long as they are not making final decisions to release product to the public or offering engineering services directly to the public (for example, software engineering consultant). However, to open a software engineering consulting practice or to claim that one is a software engineer in a formal context may now require a license in some states. For an IT worker to become licensed raises some potential legal issues, as discussed in the following paragraphs.

Negligence is defined as not doing something that a reasonable person would do or doing something that a reasonable person 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.

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 standard of measure would be higher if the defendant were an orthopedic surgeon rather than a general practitioner. In the IT arena, consider a hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed software engineer certified as an Oracle database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software.

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 might 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 not protecting a citizen from an attacker.

Professionals who breach the duty of care are liable for injuries that 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.

In the past, courts have consistently rejected attempts to sue individual parties for computer-related malpractice (see *Chatlos Systems, Inc., Plaintiff v. National Cash Register Corporation, Defendant* 479 F.Supp. 738 (1979)). Professional negligence can occur only when people fail to perform within the standards of their profession, and software engineering, until recently, was not a licensed profession in the United States. Because there were no uniform standards against which to compare a software engineer's professional behavior, he or she could not be subject to malpractice lawsuits.

CRITICAL THINKING EXERCISE: RAISING THE LEVEL OF PROFESSIONALISM AT AN IT CONSULTING FIRM

You are a member of the human resources group of an IT consulting firm with some three dozen consultants. You are considering initiating a program to encourage more of the consultants to join IT-professional organizations and to earn more IT-related certifications. Identify three business benefits of doing this. What incentives might you offer to the consultants to encourage them to join professional organizations and gain more certifications? What resistance might you expect from some of the staff? How might you overcome this resistance?

WHAT CAN BE DONE TO ENCOURAGE THE ETHICAL USE OF IT RESOURCES AMONG USERS?

This section discusses some of the most common ethical issues that IT users face, as well as ways that organizations can encourage the ethical use of IT by their employees, an area of growing concern as more companies provide employees with smartphones, tablets, and laptops—along with PCs, and other devices—to access corporate information systems, data, and the Internet.

Common Ethical Issues for IT Users

This section discusses a few common ethical issues faced by IT users. Additional ethical issues will be discussed in future chapters.

Software Piracy

As mentioned earlier in this chapter, software piracy in a corporate setting can sometimes 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. The software piracy rates in Albania, Kazakhstan, Libya, Panama, and Zimbabwe exceed 70 percent, so it is clear that business managers and IT professionals in those countries do not take a strong stand against the practice.[28]

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, if no one has paid for an additional license to use the software on the home computer, this is still piracy.

The increasing popularity of the Android smartphone operating system has created a serious software piracy problem. Some IT end users have figured out how to download applications from the Google Play store without paying for them, and then use the software or sell it to others. Indeed, the rate of software piracy for apps from Google's Play

store is alarmingly high—exceeding 90 percent for some popular games such as Monument Valley. The software piracy rate for that same game from Apple's App store is closer to 60 percent.[29] Software piracy can have a negative impact on future software development if professional developers become discouraged watching revenue from legitimate sales sink while the sales of pirated software and games skyrocket.

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular websites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at a worker's productivity and waste time. Furthermore, activities such as viewing sexually explicit material, sharing lewd jokes, and sending hate email could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment. A survey by the Fawcett Society found that one in five men admit to viewing porn at work, while a separate study found that 30 percent of mobile workers are viewing porn on their web-enabled phones.[30,31] Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describe individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also include information about customers—credit card information, telephone number, home address, and so on. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulas, 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 employee accessed a coworker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the coworker's privacy.

One of the most serious leaks of sensitive information in the U.S. history occurred in late 2010, when hundreds of thousands of leaked State Department documents were posted on the WikiLeaks' website. The source of the leaks was a low-level IT user (an army private) with access to confidential documents. The documents revealed details of behind-the-scene international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea.[32] The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will cause other countries to be less willing to share sensitive information with the United States because of concerns over further disclosures.

There have been many other instances of the breach of sensitive information by an organization's IT users. For example, a Morgan Stanley financial adviser was fired after the firm accused him of stealing the account data of almost 350,000 clients and posting some of that information for sale online. The former employee was also convicted of criminal charges, sentenced to probation, and ordered to pay restitution. In addition, Morgan Stanley paid a $1 million fine to the Securities and Exchange Commission (SEC) for its failure to protect its customers' data.[33,34]

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems; thus, 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 a policy can improve services to users, increase productivity, and reduce costs. Companies can take several actions when creating an IT usage policy, as discussed in the following sections.

Establishing Guidelines for Use of Company Hardware and 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.

Defining an Acceptable Use Policy

An **acceptable use policy (AUP)** is a document that stipulates restrictions and practices that a user must agree to in order to use organizational computing and network resources. It is an essential information security policy—so important that most organizations require that employees sign an acceptable use policy before being granted a user or network ID. An effective acceptable use policy is clear and concise and contains the following five key elements:

1. Purpose of the AUP—Why is the policy needed and what are its goals?
2. Scope—Who and what is covered under the AUP?
3. Policy—How are both acceptable use and unacceptable use defined; what are some examples of each?
4. Compliance—Who is responsible for monitoring compliance and how will compliance will be measured?
5. Sanctions—What actions will be taken against an individual who violates the policy?

Members of the legal, human resources, and information security groups are involved in creating the AUP. It is the organization's information security group that is responsible for monitoring compliance to the AUP. **Information security (infosec) group's** responsibilities include managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information, whether it is in transit, being processed, or at rest in storage.

Table 2-5 provides a manager's checklist for establishing an effective acceptable use policy. The preferred answer to each question is *yes*.

For a sample of an acceptable use policy created by SANS Institute, the largest provider of cybersecurity training and certification to professionals at governments and commercial institutions worldwide, visit *https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy*.

TABLE 2-5 Manager's checklist for establishing an acceptable use policy

Question	Yes	No
Is there a statement that explains the need for an acceptable use policy?		
Is it clear how the policy applies to the following types of workers? • Full-time employees • Part-time employees • Temps • Contractors		
Does the policy address the following issues? • Protection of the data privacy rights of employees, customers, suppliers, and others • Control of access to proprietary company data and information • Use of unauthorized or pirated software • Employee monitoring, including email, 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, excessive use of social networks, blogging, personal emailing, 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, using hard-to-guess passwords, and frequently changing passwords • The use of the computer to intimidate, harass, or insult others through abusive language in emails 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?		

Structuring Information Systems to Protect Data and Information

Organizations must implement systems and procedures that limit data access to just those 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 formulas, and staffing projections if they don't need it to do their jobs.

Installing and Maintaining a Corporate Firewall

A **firewall** is hardware or software (or a combination of both) that serves as the first line of defense between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy. A firewall can be configured to serve as an effective deterrent to unauthorized web surfing by blocking access to specific objectionable websites. (Unfortunately, the number of such sites is continually growing, so it is difficult to block them all.) A firewall can also serve as an effective barrier to incoming email from certain websites, companies, or users. It can even be programmed to

block email with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

Compliance

Compliance means to be in accordance with established policies, guidelines, specifications, or legislation. Records management software, for example, may be developed in compliance with the U.S. Department of Defense's Design Criteria Standard for Electronic Management Software applications (known as DoD 5015) that defines mandatory functional requirements for records management software used within the Department of Defense. Commercial software used within an organization should be distributed in compliance with the vendor's licensing agreement.

In the legal system, compliance usually refers to behavior in accordance with legislation—such as the Sarbanes–Oxley Act of 2002, which established requirements for a system of internal control to govern the creation and documentation of accurate and complete financial statements, or the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires employers to ensure the security and privacy of employee healthcare data. Failure to be in compliance with specific pieces of legislation can lead to criminal or civil penalties specified in that legislation.

Failure to be in compliance with legislation can also lead to lawsuits or government fines. For instance, the California Online Privacy Protection Act of 2003 requires "commercial operators of online services, including mobile and social apps, which collect personally identifiable information from Californians, to conspicuously post a privacy policy," according to the California Attorney General's office. Such a policy must outline what data are gathered, for what purposes the data are being collected, and with whom the data may be shared. Developers of mobile applications face fines of up to $2,500 for every noncompliant application that is downloaded. Several organizations, including Delta, United Airlines, and Open Table, were notified by the Attorney General's office in late 2012 that they were not in compliance and were given 30 days to provide specific plans and a timeline for becoming compliant with the law.[35]

It is a major challenge for many organizations to maintain compliance with multiple government and industry regulations, which are frequently updated and modified so that regulations have similar but sometimes conflicting requirements. For example, the California Online Privacy Protection Act of 2003 was amended in 2013 by Assembly Bill 370, which requires privacy policies to include information on how the operator responds to Do Not Track signals or similar mechanisms; the law also now requires privacy policies to state whether third parties can collect personally identifiable information about the site's users.[36]

As a result, many organizations have implemented specialized software to track and record compliance actions, hired management consultants to provide advice and training on compliance issues, and even created a new position, the chief compliance officer (CCO), to deal with compliance-related issues.

In 1972, the SEC recommended that publicly held organizations establish audit committees.[37] The **audit committee** of a board of directors provides assistance to the board in fulfilling its responsibilities with respect to the oversight of the following areas of activity:

- The quality and integrity of the organization's accounting and reporting practices and controls, including financial statements and reports
- The organization's compliance with legal and regulatory requirements

- The qualifications, independence, and performance of the company's independent auditor (a certified public accountant who provides a company with an accountant's opinion but who is not otherwise associated with the company)
- The performance of the company's internal audit team

In some cases, audit committees have uncovered violations of law and have reported their findings to appropriate law enforcement agencies.

Marvell Technology Group LTD is a Silicon Valley-based producer of semiconductors and related products. In early 2016, the firm launched an audit committee investigation that scrutinized financial results for several quarters. The audit committee uncovered that in some cases Marvell personnel, IT users, would ask customers to accept delivery of products sooner than they had requested allowing the company to book revenue in earlier quarters. Such transactions were made in response to "significant pressure" from the management on sales teams to meet revenue targets. Such sales reporting accounted for about 9 percent of first quarter revenue in fiscal 2016 and 11 percent for the second quarter. Facing pressure from investors, both the firm's chief executive and its president were fired. In their first conference call with investors, the firm's new management team pledged to discontinue the practice of booking revenue prematurely.[38]

In addition to an audit committee, most organizations also have an internal audit department whose primary responsibilities include the following:

- Determine that internal systems and controls are adequate and effective
- Verify the existence of company's assets and maintain proper safeguards over their protection
- Measure the organization's compliance with its own policies and procedures
- Ensure that institutional policies and procedures, appropriate laws, and good practices are followed
- Evaluate the adequacy and reliability of information available for management decision making

Although the members of the internal audit team are not typically experts in detecting and investigating financial statement fraud, they can offer advice on how to develop and test policies and procedures that result in transactions being recorded in accordance with generally accepted accounting principles (GAAP). This can go a long way toward deterring fraud related to an organization's financial statements. Quite often in cases of financial statement fraud, senior management (including members of the audit committee) ignored or tried to suppress the recommendations of the internal audit team, especially when red flags were raised.

CRITICAL THINKING EXERCISE: CREATING AN AUP

You are a new member of the infosec group for a midsized consumer products manufacturing organization. After you have been there a few weeks, you are shocked to learn that the organization has not defined an AUP. You are determined to prioritize the creation of such a policy for the infosec group. What key points can you make to management to justify the necessary time and effort to create an AUP? Who else should you recruit in your efforts to sell this idea to management? Identify the key points that should be included in the AUP.

Summary

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

- An IT worker must maintain good working relationships with employers, clients, suppliers, other professionals, IT users, and society at large. Each relationship has its own set of ethical issues and potential problems.
- In relationships between IT workers 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 workers and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project. The IT worker must remain objective and guard against any sort of conflict of interest, fraud, misrepresentation, or breach of contract.
- A major goal for IT workers and suppliers is to develop good working relationships in which no action can be perceived as unethical.
- Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage.
- Internal control is the process established by an organization's board of directors, managers, and IT group to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.
- Policies are the guidelines, standards, and laws by which the organization must abide. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process.
- A fundamental concept of good internal control is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people.
- The 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 and to any company with shares listed on any U.S. stock exchange.
- In relationships between IT workers and other professionals, the priority is to improve the profession through activities such as mentoring inexperienced colleagues, demonstrating professional loyalty, and avoiding résumé inflation and the inappropriate sharing of corporate information.
- 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 workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.

What can be done to encourage the professionalism of IT workers?

- A professional is one who possess the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well.
- A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.
- IT workers of all types can improve their profession's reputation for professionalism by (1) subscribing to a professional code of ethics, (2) joining and participating in professional organizations, (3) obtaining appropriate certifications, and (4) supporting government licensing where available.
- A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group.
- Codes of ethics usually 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. The codes also typically include a commitment to continuing education for those who practice the profession.
- Adherence to a code of ethics can produce many benefits for the individual, the profession, and society as a whole, including ethical decision making, high standards of practice and ethical behavior, trust and respect with the general public, and access to an evaluation benchmark that can be used for self-assessment.
- Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.
- Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.
- Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Numerous companies and professional organization offer certification.
- Most states support the licensing of software engineers, and the state licensing boards have ultimate responsibility over specific requirements for licensing in their jurisdiction.

What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

- IT users face several common ethical issues, including software piracy, inappropriate use of computing resources, and inappropriate sharing of information.
- Actions that can be taken to encourage the ethical behavior of IT users include establishing guidelines for the use of company hardware and software; defining an AUP for the use of IT resources; structuring information systems to protect data and information; installing and maintaining a corporate firewall; and ensuring compliance with laws, policies, and standards.
- The information security (infosec) group is responsible for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information.
- The audit committee of a board of directors and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Key Terms

acceptable use policy (AUP)
audit committee
body of knowledge
breach of contract
breach of the duty of care
bribery
BSA | The Software Alliance (BSA)
certification
compliance
conflict of interest
duty of care
firewall
Foreign Corrupt Practices Act (FCPA)
fraud
government license
information security (infosec) group
internal control
IT user
material breach of contract
misrepresentation
negligence
policy
procedure
process
professional code of ethics
professional malpractice
reasonable person standard
reasonable professional standard
résumé inflation
separation of duties
Software & Information Industry Association (SIIA)
software engineer
trade secret
whistle-blowing

Self-Assessment Questions

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

1. An IT worker cannot be sued for professional malpractice unless he or she is licensed. True or False.
2. The mission of the Software & Information Industry Association and the Business Software Alliance is to _____.
   a. protect the trade secrets of world's largest software and hardware manufacturers
   b. encourage disgruntled employees to report misdeeds by their employers
   c. stop the unauthorized copying of software produced by its members
   d. provide recommendations on how to develop software code that is unhackable
3. _____ 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.