CHAPTER 2

ETHICS FOR IT WORKERS AND IT USERS

QUOTE

This above all: to thine own self be true.
—William Shakespeare, playwright

VIGNETTE

New York City Payroll Project Riddled with Fraud

The CityTime project was meant to replace a largely manual, paper-based payroll system for the city of New York (NYC). The goal was to provide a tool that would help city administrators manage a workforce of over 100,000 employees spread across 63 departments. It was also intended to simplify the employee time-reporting process, which was complicated by numerous union timekeeping rules, and to identify employees who tried to fraudulently inflate their paychecks. The project was initiated in 1998 when the city awarded the contract to a subsidiary of MCI, a telecommunications company that later ran into financial scandals and, ultimately, filed for bankruptcy.[1]

In 2001, the CityTime contract was reassigned to Science International Applications Incorporated (SAIC), a defense company. In an unusual move, the handoff to SAIC occurred without the contract going through the normal competitive bidding process required for contracts of this size. Around the same time, Spherion Atlantic Enterprises was hired as a subcontractor to provide quality assurance

on the CityTime project, with an initial contract of $3.4 million. The city's contract with Spherion was eventually revised 11 times, with a resulting cost of $48 million.[2]

Richard Valcich, the NYC payroll office executive director during the initial years of the project, accused SAIC of dragging its feet on the project and was skeptical of the company's ability to deliver a quality product. However, Valcich retired in 2004 and was replaced by Joel Bondy, a staunch advocate of the project.[3] In this role, Bondy was responsible for overseeing and re-awarding Spherion's contract. It was later discovered that Bondy worked for Spherion for two years prior to joining the city.

In another questionable move, the CityTime contract was switched from a fixed-price contract to a "time and materials" contract, and the project costs spiraled out of control—from $224 million in 2006 to $628 million by 2009. This switch in the terms of the contract plus lack of project oversight made it even easier for those involved with the project to commit fraud.[4]

At a city hearing in December 2010, Bondy revealed that Spherion employees were billing the city at a rate of $236.25 per hour and that a number of former city employees had become Spherion employees.[5] Mr. Bondy resigned shortly after this meeting.[6]

That same month, federal prosecutors charged several consultants for the CityTime project with a multimillion dollar fraud scheme, which allegedly started in 2005. The consultants were accused of manipulating the city into paying for contracts to businesses that the consultants controlled, and then redirecting part of the money to enrich themselves personally.[7]

In May 2011, federal investigators arrested Gerald Denault, the senior project manager at SAIC, for allegedly receiving over $5 million in kickbacks and for committing wire fraud and money laundering. Denault had convinced his employer to hire TechnoDyne LLC as the main subcontractor for the

project. TechnoDyne eventually received $450 million out of the $600 million paid to SAIC and siphoned off millions to a bogus India-based consulting firm owned by Denault.[8] The two owners of TechnoDyne are now fugitives and their whereabouts are unknown. Six other defendants are scheduled to go to trial in 2013.[9]

In March 2012, SAIC agreed to pay $500 million to avoid prosecution for its role in the CityTime scandal; most of that money was to go back to the city of New York. By this time, it was estimated that NYC had paid out $652 million—with an outstanding bill of $41 million—owed on the project, which was originally estimated to cost $63 million and to be completed in 2003.[10]

Questions to Consider

1. What were some early warning signs that signaled things were not going well with the CityTime project?
2. What steps should city managers and SAIC have taken at an early stage of the project to identify and prevent fraud?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key characteristics distinguish a professional from other kinds of workers, and is an IT worker considered a professional?
2. What factors are transforming the professional services industry?
3. What relationships must an IT worker manage, and what key ethical issues can arise in each?
4. How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
5. What is meant by compliance, and how does it help promote the right behaviors and discourage undesirable ones?

IT PROFESSIONALS

A **profession** is a calling that requires specialized knowledge and often long and intensive academic preparation. Over the years, the United States government adopted labor laws and regulations that required a more precise definition of what is meant by a *professional*

employee. The United States Code of federal regulations defines a "professional employee" as one who is engaged in the performance of work:

> "(i) 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 in an institution of higher learning or a hospital (as distinguished from knowledge acquired by a general academic education, or from an apprenticeship, or from training in the performance of routine mental, manual, mechanical, or physical activities);
> (ii) requiring the consistent exercise of discretion and judgment in its performance;
> (iii) which is predominantly intellectual and varied in character (as distinguished from routine mental, manual, mechanical, or physical work); and
> (iv) which is of such character that the output produced or the result accomplished by such work cannot be standardized in relation to a given period of time."[11]

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 assist other professionals in their development. In addition, many professional roles carry special rights and responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information while maintaining doctor–patient confidentiality.

✓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 such as mobile application developers, software engineers, systems analysts, and network administrators. 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 United States Code. From a *legal* perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as 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 workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large—as illustrated in Figure 2-1. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

FIGURE 2-1 Professional relationships IT workers must manage
Credit: Course Technology/Cengage Learning

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 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. These issues may include protection of company secrets, vacation policy; time off 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 as the need arises (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 aspects 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.

Zynga is a provider of online social games such as ChefVille, CityVille, FarmVille, FrontierVille, and Zynga Poker that boast over 300 million active monthly users.[14] After just over a year with Zynga, the firm's general manager of CityVille left to become a vice president at Kixeye, a competitor. Zynga claimed that the employee stole files with data critical to the business—including financial projections, marketing plans, and game designs.[15] Zynga filed a request for a temporary restraining order barring its former employee from sharing or copying the information or from engaging in any actions using the information to develop online games employing these trade secrets.

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 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.

The H-1B visa is a work visa that allows foreigners to come to the United States and work full-time in specialty occupations that require at least a four-year bachelor's degree in a specific field. A U.S. consultant for India-based outsourcing firm Infosys filed a whistle-blower lawsuit against the firm for abusing H-1B program rules. The lawsuit alleged that at a management meeting in Bangalore, Infosys officials discussed the need to "creatively" circumvent the H-1B visa restrictions. The lawsuit further alleged that Infosys brought workers to the United States on B-1 visas (which are intended for workers coming to the United States for short-term work assignments only), but that these workers were assigned full-time jobs. It also claimed that Infosys was not paying the B-1 workers the prevailing wage and was not withholding federal and state income taxes.[16] The whistle-blower filed a separate lawsuit in which he claimed that Infosys retaliated against him for the filing of the visa-related lawsuit by lowering his bonuses, harassing him, and giving him no meaningful work to do.[17]

Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same organization as the IT worker. In other cases, the client is part of a different organization. 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 client and 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 interests of the client. 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 whether its recommendations can be trusted.

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.

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.

As an example of alleged fraud, consider the case of Paul Ceglia, who in 2010 sued Facebook claiming to own a majority of the company. Ceglia claimed that he signed a contract with Mark Zuckerberg in 2003 to design and develop the Web site that eventually became Facebook. He alleged that he paid Zuckerberg $1,000 for the programming work and also invested an additional $1,000 in Zuckerberg's Facebook project in exchange for a 50 percent interest in Facebook.[18] Facebook lawyers have asserted that the lawsuit is an outright fraud and have depositions alleging that "Ceglia manufactured evidence, including purported emails with Zuckerberg, to support his false claim to an interest in Facebook" and that "Ceglia destroyed evidence that was inconsistent with his false claim." Facebook's attorneys pointed out that Zuckerberg did not even conceive of Facebook until eight

months after Zuckerberg did the contract work (which, they say, was completely unrelated to Facebook) for Ceglia. They further alleged that Ceglia's emails to Zuckerberg were manufactured to support his claims. Eventually, Ceglia was arrested on federal mail and wire fraud charges.[19]

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.

Siri, the voice-activated software that comes with the Apple iPhone, has delighted many iPhone users; however, not everyone has had a positive experience. Shortly after one user in New York purchased an iPhone 4S, he realized that Siri was not performing as expected. When he asked Siri for directions, it did not understand the question or after a long delay gave incorrect directions. As a result, the user filed a lawsuit against Apple claiming that advertising for the Siri amounted to "intentional misrepresentation" and that Apple's claims about the Siri software were "misleading and deceptive." Attorneys for this user are considering turning the case into a class action against Apple.[20]

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 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."[21]

In an out-of-court settlement of a breach of contract lawsuit brought by the General Services Administration (GSA), Oracle Corporation agreed to pay the federal agency $200 million. Oracle entered into a contract with the GSA for the sale of software and technical support to various departments of the federal government. The contract required Oracle to provide the government with its pricing policies. The lawsuit arose when the GSA claimed that Oracle "knowingly failed to meet its contractual obligations to provide GSA with current, accurate, and complete information about its commercial sales practices, including discounts offered to other customers, and that Oracle knowingly made false statements to GSA about its sales practices and discounts." The GSA further claimed that Oracle failed to disclose that other customers received greater discounts than the GSA and that, based on its contract with Oracle, those discounts should have been passed on to the GSA.[22]

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. Consider the following frequent causes of problems in IT projects:

- The customer changes the scope of the project or the system requirements.
- Poor communication between customer and vendor leads 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.

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.

A former midlevel supply chain manager at Apple pled guilty in 2011 to taking over $1 million in payments from certain iPhone, iPad, and iPod suppliers in China, Singapore, South Korea, and Taiwan. The kickbacks took place over several years and were in exchange for the employer providing confidential information about Apple's production plans, enabling the suppliers to negotiate more favorable deals with Apple. He now faces 20 years in prison on charges of money laundering, receiving kickbacks, and wire fraud.[23]

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. 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 whose securities are listed in the United States to meet U.S. 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 must be frequently audited by both 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).[24]

There is growing global recognition of the need to prevent corruption. The United Nations Convention Against Corruption is a legally binding global treaty designed to fight bribery and corruption. During its November 2010 meeting, Finance Ministers and Central Bank Ministers of members of the Group of 20 (G20), which includes Argentina, China, India, Japan, Russia, the United Kingdom, the United States, and 13 other countries, pledged to implement this treaty effectively. In particular, the countries pledged to put in place mechanisms for the recovery of property from corrupt officials through international cooperation in tracing, freezing, and confiscating assets. Members also pledged to adopt and enforce laws against international bribery and put in place rules to protect whistleblowers.[25]

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 some 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

Source Line: Course Technology/Cengage Learning

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.

Yahoo! hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012.[26] Just four months later, Thompson left the company, due, at least in part, to revelations that his résumé falsely claimed that he had earned a bachelor's degree in computer science.[27]

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.[28] Résumé inflation is an even bigger problem in Asia. According to a recent survey conducted by the University of Hong Kong and a Hong Kong–based company specializing in preemployment screening, over 62 percent of respondents confessed to exaggerating their years of experience, previous positions held, and job responsibilities; 33 percent confessed to having exaggerated even more.[29] 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	How to uncover the truth
Dates of employment	Thorough reference check
Job title	Thorough reference check
Criminal record	Criminal background check
Inflated salary	Thorough reference check
Education	Verification of education claims with universities and other training organizations
Professional licenses	Verification of license with accrediting agency
Working for fictitious company	Thorough background check

Source Line: Lisa Vaas, "Most Common Resume Lies," The Ladders, July 17, 2009, www.theladders.com/career-advice/most-common-resume-lies.

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.

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. IT workers 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.

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.