Common Ethical Issues for IT Users

This section focuses on encouraging employees' ethical use of IT, which is an area of growing concern as more companies provide employees with PCs, tablets, cellphones, and other devices to access to corporate information systems, data, and the Internet. A few common ethical issues for IT users are discussed here.

Software Piracy

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. For example, the software piracy rate in China exceeds 80 percent, so it is clear that the business managers and IT professionals in that country do not take a strong stand against the practice. Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home. When confronted, the IT user's argument might be: "I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work." However, 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 Android Market Web site without paying for them, and then use the software or sell it to others. One legitimate Android application developer complained that his first application was

pirated within a month and that the number of downloads from the pirate's site were greater than his own. Professional developers become discouraged as they watch their sales sink while pirates' sales rocket.

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at worker productivity and waste time. Furthermore, 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 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. Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders. Recently, the executive director of the Pentagon's Missile Defense Agency issued a memo to its 8,000 employees warning them to stop using their work computers to access Internet porn sites. One concern of government officials is that many pornography sites are infected with computer viruses and other malware; criminals and foreign intelligence agencies often use such sites as a means to gain access to government and corporate computer networks. For example, a foreign agent can embed malware capable of stealing data or opening computer communications ports whenever certain photos or videos are downloaded to a computer.

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also includes 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 unintentionally, 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. In late 2010, hundreds of thousands of leaked State Department documents were posted on the WikiLeaks Web site. As of this writing, it appears that 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-scenes international diplomacy, often disclosing candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea. The leaked documents strained relations between the United States and some of its allies.