**People as Part of an Information System**

While most everyone agrees that technology has had a very positive impact on people, it is important to recognize the negative, or potentially negative, impacts as well. Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects. The most significant concerns are

• **Privacy:** What are the threats to personal privacy and how can we protect ourselves?

• **Security:** How can access to sensitive information be controlled and how can we secure hardware and software?

• **Ethics:** How do the actions of individual users and companies affect society?

Let us begin by examining privacy.

**Privacy**

As you have seen, computing technology makes it possible to collect and use data of all kinds, including information about people. The Web sites you visit, the stores where you shop, and the television shows you watch are all examples of information about you. How would you feel if you learned such information was being collected or shared? Would it matter who was collecting it, or how it was being used, or whether it was even correct?

**Privacy** concerns the collection and use of data about individuals. There are three primary privacy issues:

*•* ***Accuracy*** relates to the responsibility of those who collect data to ensure that the data is correct.

*•* ***Property*** relates to who owns data and rights to software.

*•* ***Access*** relates to the responsibility of those who have data to control and who is able to use that data.

**Security**

We are all concerned with having a safe and secure environment to live in. We are careful to lock our car doors and our homes. We are careful about where we walk at night and whom we talk to. This is personal security. What about computer security? What if someone gains unauthorized access to our computer or other computers that contain information about us? What if someone steals our computer or other computers that contain information about us? What are the major threats to computer security, and how can we be protected?

**Computer Criminals**

A **computer crime** is an illegal action in which the perpetrator uses special knowledge of computer technology. Typically, computer criminals are either employees, outside users, hackers, crackers, organized crime members, or terrorists.

• **Employees:** The largest category of computer criminals consists of those with the easiest access to computers – namely, employees. Sometimes the employee is simply trying to steal something from the employer – equipment, software, electronic funds, proprietary information, or computer time. Sometimes the employee is acting out of resentment and is trying to get back at the company.

• **Outside users:** Not only employees but also some suppliers or clients may have access to a company’s computer system. Examples are bank customers who use an automated teller machine. Like employees, these authorized users may be able to obtain confidential passwords or find other ways of committing computer crimes.

• **Hackers and crackers: Hackers** are people who create or improve programs and share those programs with fellow hackers. Typically, they are not criminals. **Crackers,** on the other hand, create and share programs designed to gain unauthorized access to computer systems or disrupt networks. Their motives are malicious and can be very destructive and costly. Typically, they are criminals.

• **Organized crime:** Members of organized crime groups have discovered that they can use computers just as people in legitimate businesses do, but for illegal purposes. For example, computers are useful for keeping track of stolen goods or illegal gambling debts. In addition, counterfeiters and forgers use microcomputers and printers to produce sophisticated-looking documents such as checks and driver’s licenses.

• **Terrorists:** Knowledgeable terrorist groups and hostile governments could potentially crash satellites and wage economic warfare by disrupting navigation and communication systems. The Department of Defense reports that its computer systems are probed approximately 250,000 times a year by unknown sources.

**Ethics**

The essential element that controls how computers are used today is *ethics.*

**Ethics,** as you may know, are standards of moral conduct. **Computer ethics** are guidelines for the morally acceptable use of computers in our society. We are all entitled to ethical treatment. This includes the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands. These issues, largely under the control of corporations and government agencies, were covered earlier in this chapter. Now we’ll examine two important issues in computer ethics where average users have a role to play.

**Copyright** is a legal concept that gives content creators the right to control use and distribution of their work. Materials that can be copyrighted include paintings, books, music, films, and even video games. Some users choose to make unauthorized copies of digital media, which violates copyright. For example, making an unauthorized copy of a digital music file for a friend might be a copyright violation.

***Software piracy*** is the unauthorized copying and distribution of software. The software industry loses over $30 billion annually to software privacy. Two related topics are the Digital Millennium Copyright Act and digital rights management.

• **Digital Millennium Copyright Act** establishes the right of a program owner to make a backup copy of any program and disallows the creation of copies to be sold or given away. It is also illegal to download copyright-protected music and videos from the Internet.

• **Digital rights management (DRM)** is a collection of technologies designed to prevent copyright violations. Typically, DRM is used to (1) control the number of devices that can access a given file as well as (2) limit the kinds of devices that can access a file.

Another ethical issue is ***plagiarism*,** which means representing some other person’s work and ideas as your own without giving credit to the original source. Although plagiarism was a problem long before the invention of computers, computer technology has made plagiarism easier. For example, simply cutting and pasting content from a Web page into a report or paper may seem tempting to an overworked student or employee. Correspondingly, computer technology has made it easier than ever to recognize and catch plagiarists.

**CONCEPT CHECK**

1. What is the distinction between ethics and computer ethics?

2. Define copyright, software privacy, the Digital Millennium Copyright Act, and digital rights management.

3. What is plagiarism?