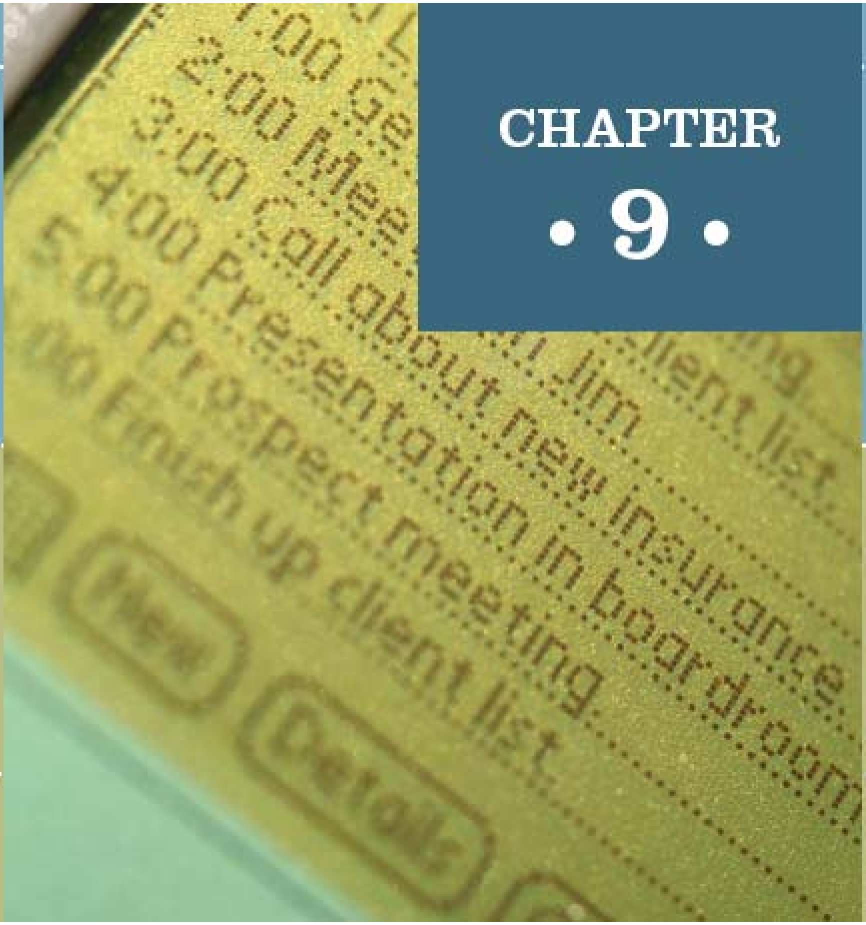


CHAPTER

• 9 •

Security, Privacy, and Ethical Issues in Information Systems and the Internet

Fundamentals of Information Systems

Third Edition

Principles and Learning Objectives

- Policies and procedures must be established to avoid computer waste and mistakes.
  - Describe some examples of waste and mistakes in an IS environment, their causes, and possible solutions.
  - Identify policies and procedures useful in eliminating waste and mistakes.

Principles and Learning Objectives (continued)

- Computer crime is a serious and rapidly growing area of concern requiring management attention.
  - Explain the types and effects of computer crime.
  - Identify specific measures to prevent computer crime.
  - Discuss the principles and limits of an individual's right to privacy.

Principles and Learning Objectives (continued)

- Working conditions must be designed to avoid negative ethical consequences.
  - Outline criteria for the ethical use of information systems.

Computer Waste and Mistakes

- Computer waste
  - The inappropriate use of computer technology and resources
- Computer-related mistakes
  - Errors, failures, and other computer problems that make computer output incorrect or not useful

Computer Waste

- Discarding of technology
- Unused systems
- Personal use of corporate time and technology
- Spam

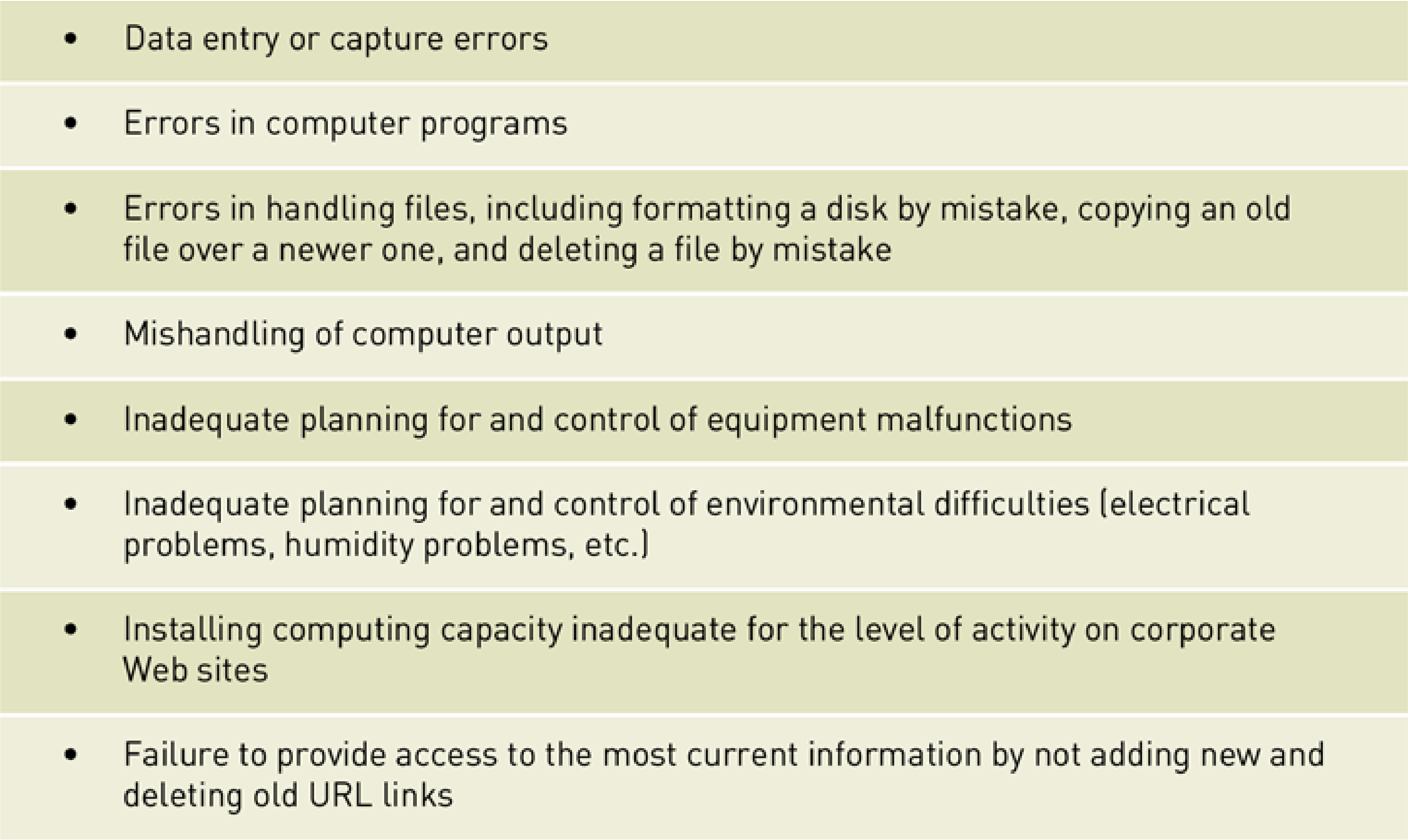
Computer-Related Mistakes

- Mistakes can be caused by unclear expectations and a lack of feedback
- A programmer might develop a program that contains errors
- A data-entry clerk might enter the wrong data

Preventing Computer-Related Waste and Mistakes

- Establishing policies and procedures
- Implementing policies and procedures
- Monitoring policies and procedures
- Reviewing policies and procedures

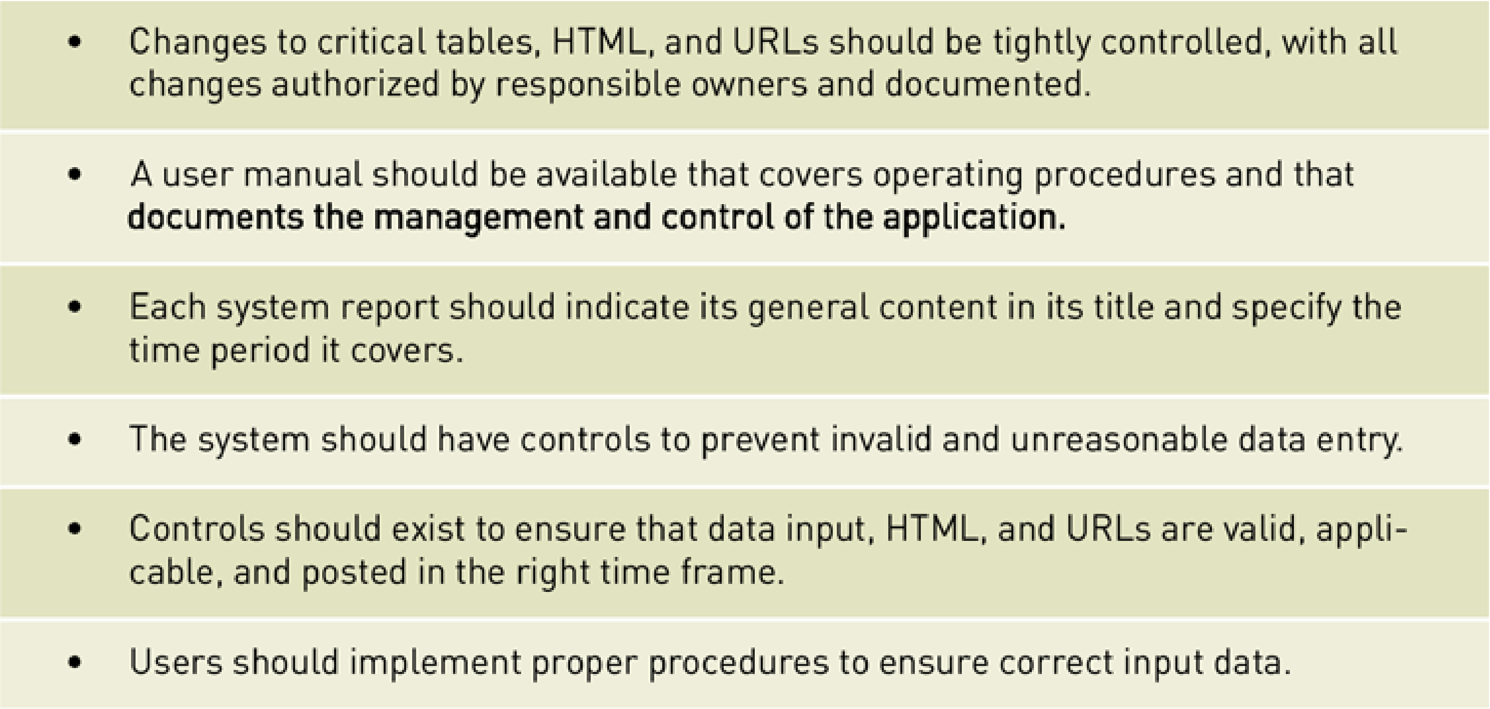
Establishing Policies and Procedures



- Data entry or capture errors
- Errors in computer programs
- Errors in handling files, including formatting a disk by mistake, copying an old file over a newer one, and deleting a file by mistake
- Mishandling of computer output
- Inadequate planning for and control of equipment malfunctions
- Inadequate planning for and control of environmental difficulties (electrical problems, humidity problems, etc.)
- Installing computing capacity inadequate for the level of activity on corporate Web sites
- Failure to provide access to the most current information by not adding new and deleting old URL links

Table 9.2: Types of Computer-Related Mistakes

Implementing Policies and Procedures



- Changes to critical tables, HTML, and URLs should be tightly controlled, with all changes authorized by responsible owners and documented.
- A user manual should be available that covers operating procedures and that **documents the management and control of the application.**
- Each system report should indicate its general content in its title and specify the time period it covers.
- The system should have controls to prevent invalid and unreasonable data entry.
- Controls should exist to ensure that data input, HTML, and URLs are valid, applicable, and posted in the right time frame.
- Users should implement proper procedures to ensure correct input data.

Table 9.3: Useful Policies to Eliminate Waste and Mistakes

Computer Crime

- Often defies detection
- The amount stolen or diverted can be substantial
- The crime is “clean” and nonviolent
- The number of IT-related security incidents is increasing dramatically
- Computer crime is now global

Computer Crime (continued)

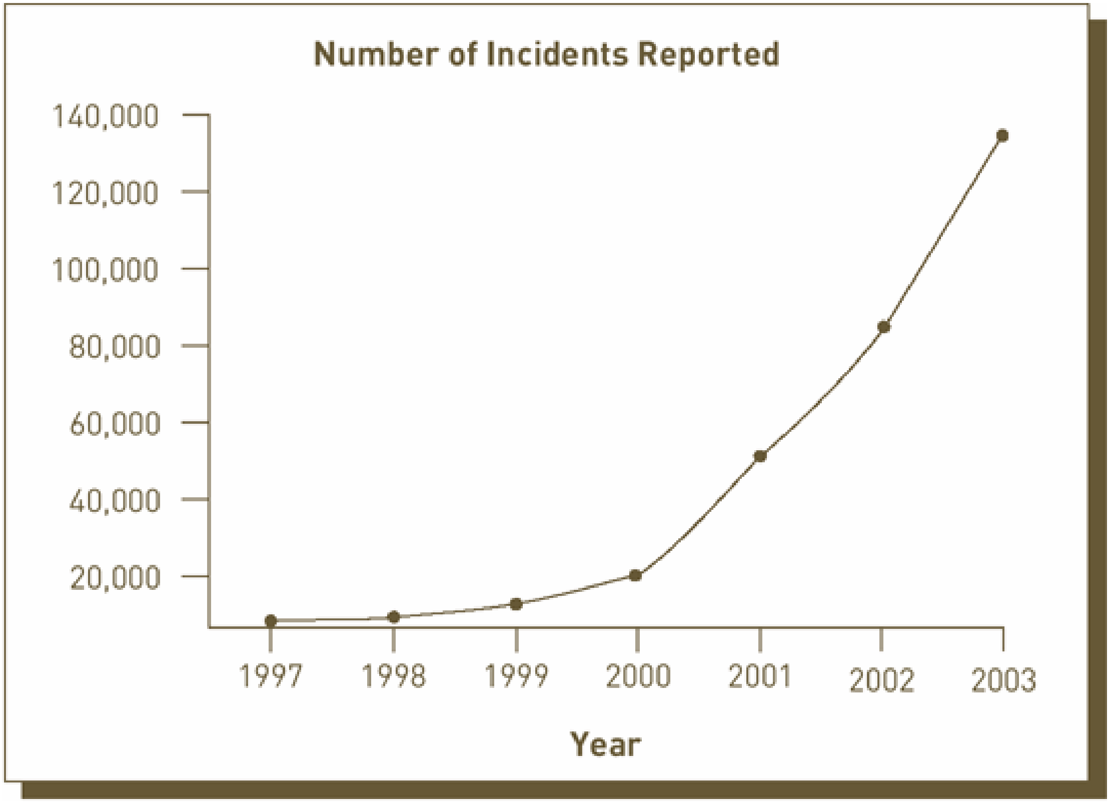


Figure 9.1: Number of Incidents Reported to CERT

The Computer as a Tool to Commit Crime

- Criminals need two capabilities to commit most computer crimes:
  - Knowing how to gain access to the computer system
  - Knowing how to manipulate the system to produce the desired result
- Social engineering
- Dumpster diving

Cyberterrorism

- **Cyberterrorist:** intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attacks against computers, networks, and the information stored on them
- Homeland Security Department's Information Analysis and Infrastructure Protection Directorate

Identity Theft

- An imposter obtains key pieces of personal identification information, such as Social Security or driver’s license numbers, in order to impersonate someone else
- The information is then used to obtain credit, merchandise, and services in the name of the victim or to provide the thief with false credentials
- Identity Theft and Assumption Deterrence Act of 1998

The Computer as the Object of Crime

- Illegal access and use
- Data alteration and destruction
- Information and equipment theft

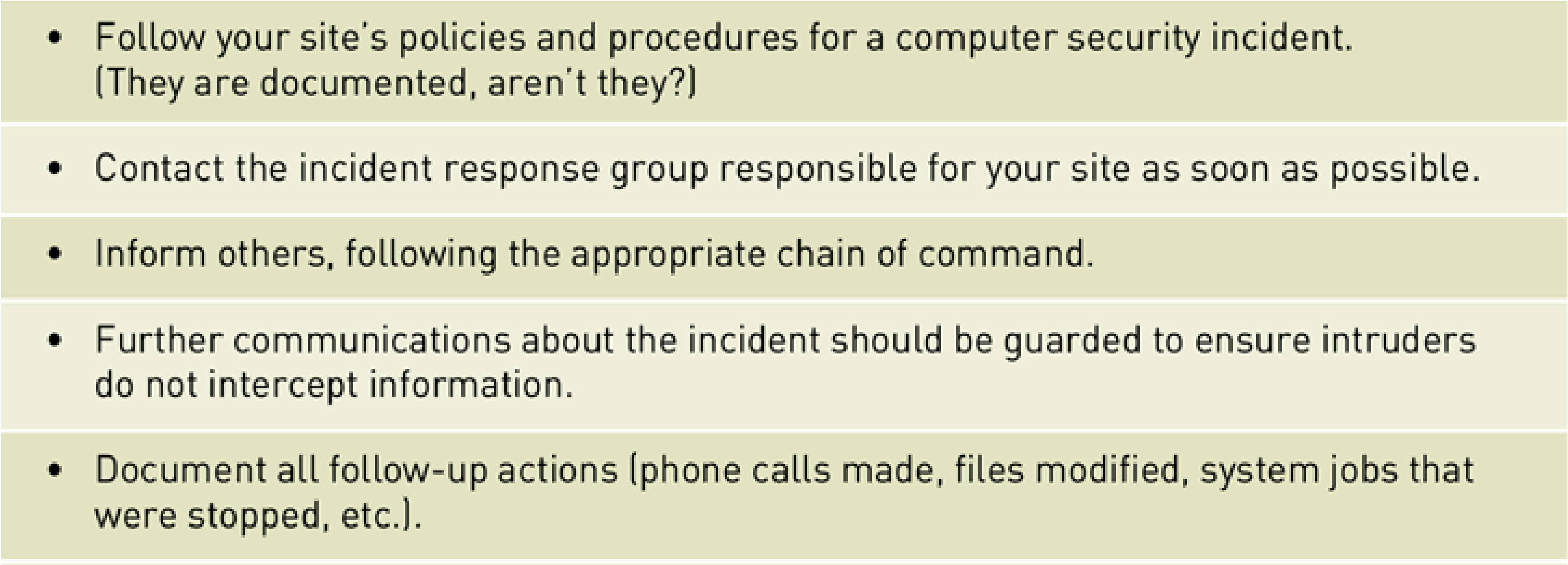
The Computer as the Object of Crime (continued)

- Software and Internet piracy
- Computer-related scams
- International computer crime

Illegal Access and Use

- Hackers
- Criminal hackers (also called crackers)
- Script bunnies
- Insiders

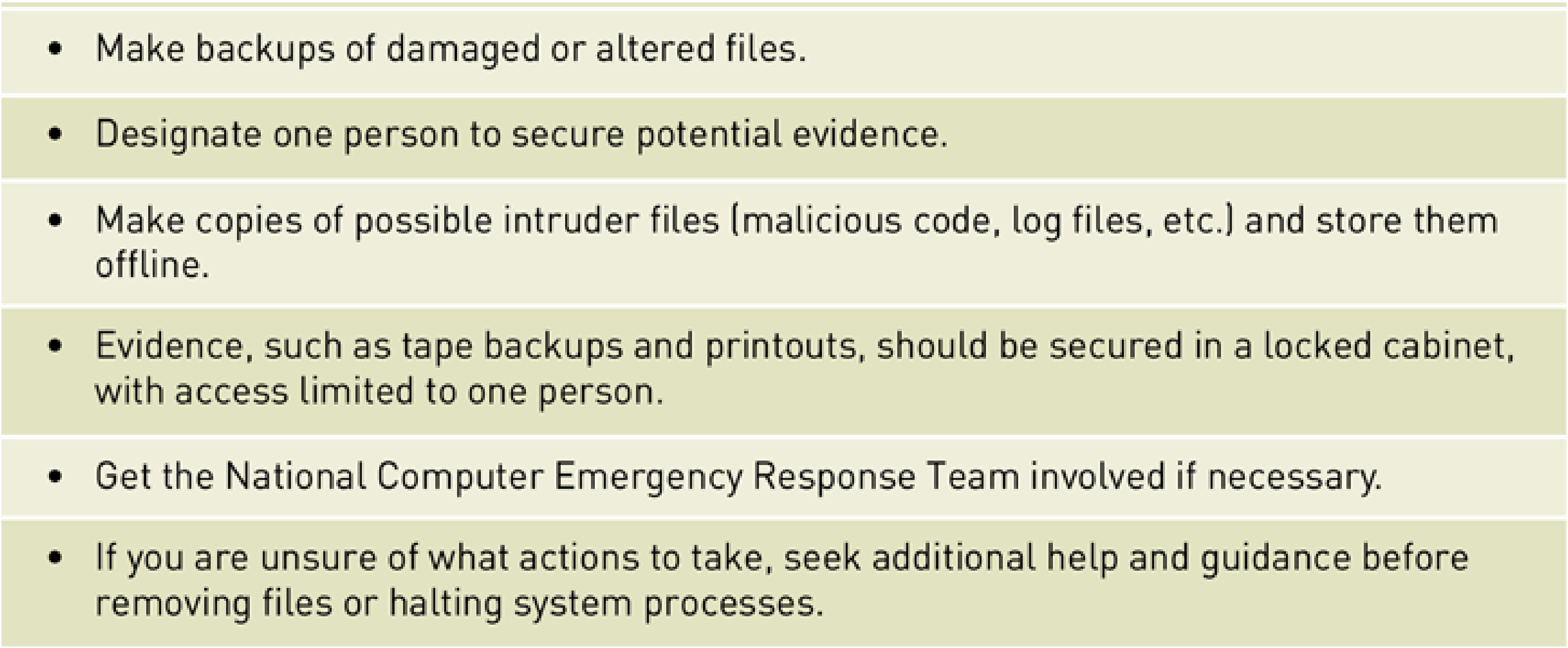
Illegal Access and Use (continued)



- Follow your site's policies and procedures for a computer security incident. (They are documented, aren't they?)
- Contact the incident response group responsible for your site as soon as possible.
- Inform others, following the appropriate chain of command.
- Further communications about the incident should be guarded to ensure intruders do not intercept information.
- Document all follow-up actions (phone calls made, files modified, system jobs that were stopped, etc.).

Table 9.4: How to Respond to a Security Incident

Illegal Access and Use (continued)



- Make backups of damaged or altered files.
- Designate one person to secure potential evidence.
- Make copies of possible intruder files (malicious code, log files, etc.) and store them offline.
- Evidence, such as tape backups and printouts, should be secured in a locked cabinet, with access limited to one person.
- Get the National Computer Emergency Response Team involved if necessary.
- If you are unsure of what actions to take, seek additional help and guidance before removing files or halting system processes.

Table 9.4: How to Respond to a Security Incident (continued)

Data Alteration and Destruction

- **Virus:** a computer program capable of attaching to disks or other files and replicating itself repeatedly, typically without the user's knowledge or permission
- **Worm:** an independent program that replicates its own program files until it interrupts the operation of networks and computer systems

Data Alteration and Destruction (continued)

- **Trojan horse:** a program that appears to be useful but actually masks a destructive program
- **Logic bomb:** an application or system virus designed to “explode” or execute at a specified time and date

Using Antivirus Programs

- **Antivirus program:** program or utility that prevents viruses and recovers from them if they infect a computer
- An antivirus software should be run and updated often

Information and Equipment Theft

- To obtain illegal access, criminal hackers require identification numbers and passwords
  - Password sniffer
- Theft of data and software
- Theft of computer systems and equipment

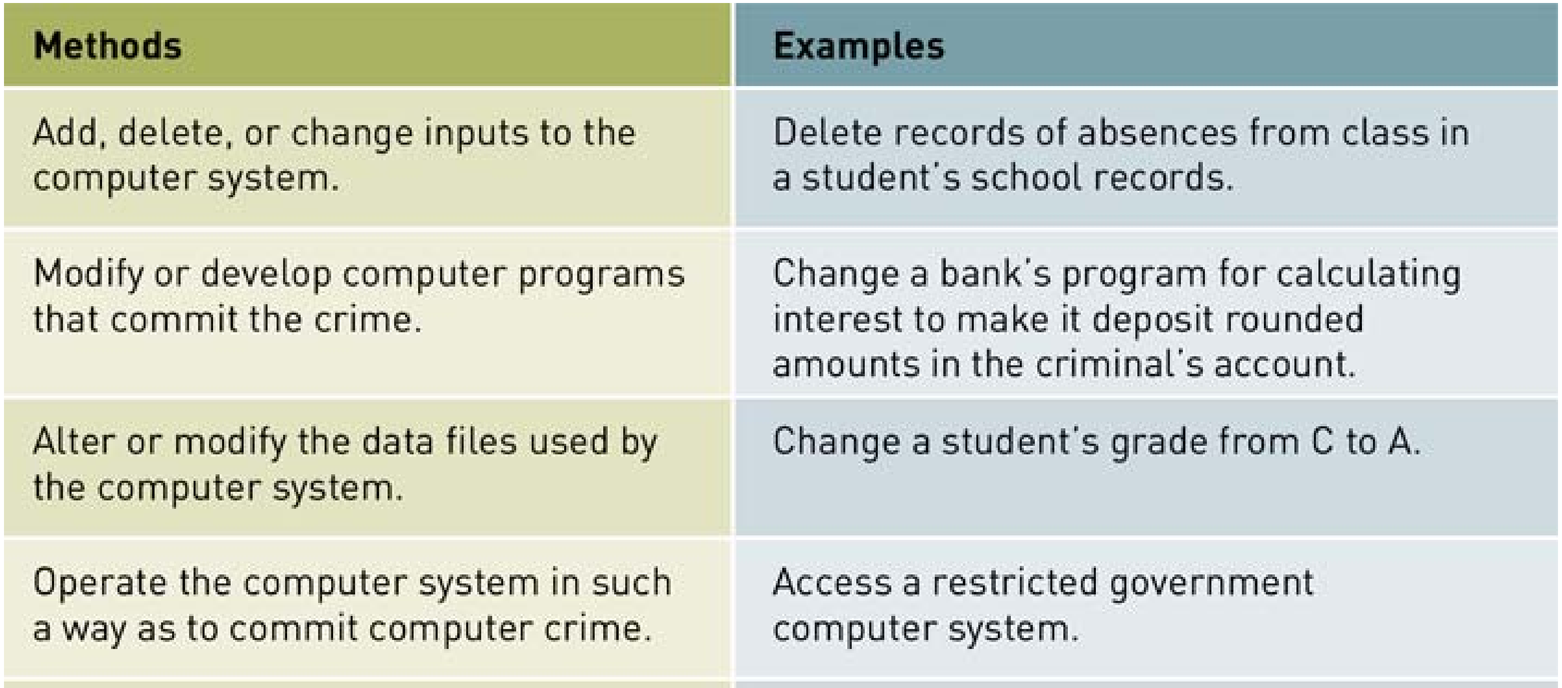
Software and Internet Software Piracy

- **Software piracy:** the act of illegally duplicating software
- **Internet software piracy:** illegally downloading software from the Internet

Preventing Computer-Related Crime

- Crime prevention by state and federal agencies
- Crime prevention by corporations
  - **Public key infrastructure (PKI):** a means to enable users of an unsecured public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority
  - **Biometrics:** the measurement of one of a person’s traits, whether physical or behavioral

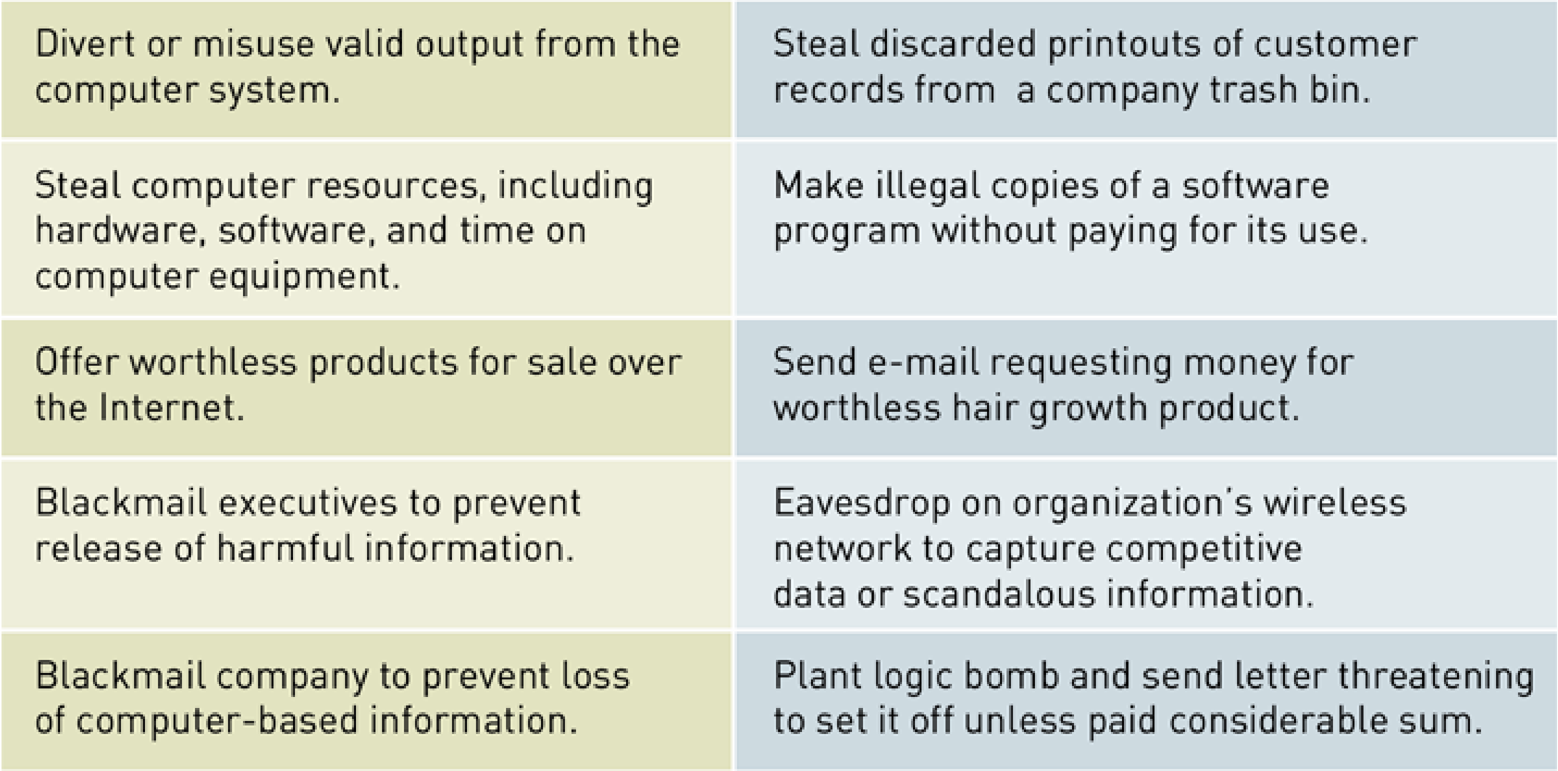
Preventing Computer-Related Crime (continued)



Methods	Examples
Add, delete, or change inputs to the computer system.	Delete records of absences from class in a student's school records.
Modify or develop computer programs that commit the crime.	Change a bank's program for calculating interest to make it deposit rounded amounts in the criminal's account.
Alter or modify the data files used by the computer system.	Change a student's grade from C to A.
Operate the computer system in such a way as to commit computer crime.	Access a restricted government computer system.

Table 9.8: Common Methods Used to Commit Computer Crimes

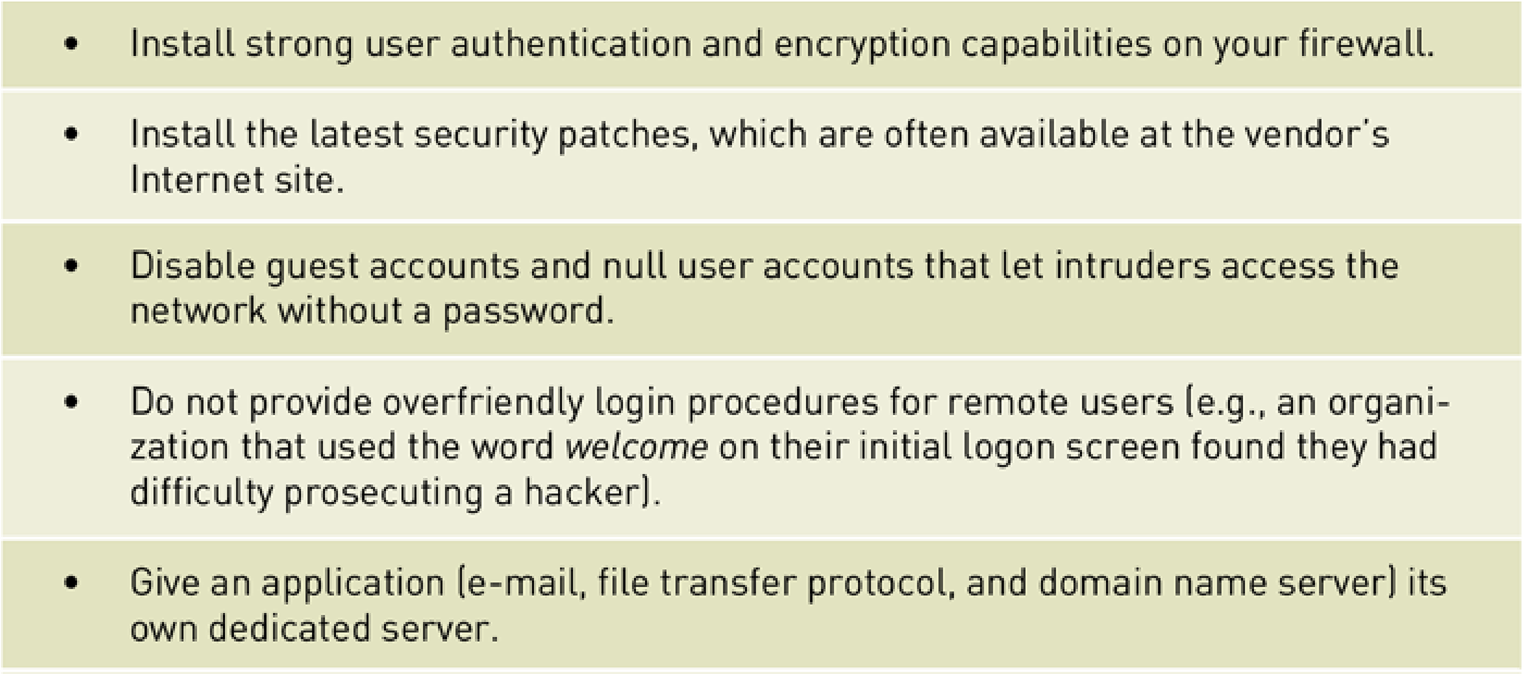
Preventing Computer-Related Crime (continued)



Divert or misuse valid output from the computer system.	Steal discarded printouts of customer records from a company trash bin.
Steal computer resources, including hardware, software, and time on computer equipment.	Make illegal copies of a software program without paying for its use.
Offer worthless products for sale over the Internet.	Send e-mail requesting money for worthless hair growth product.
Blackmail executives to prevent release of harmful information.	Eavesdrop on organization's wireless network to capture competitive data or scandalous information.
Blackmail company to prevent loss of computer-based information.	Plant logic bomb and send letter threatening to set it off unless paid considerable sum.

Table 9.8: Common Methods Used to Commit Computer Crimes (continued)

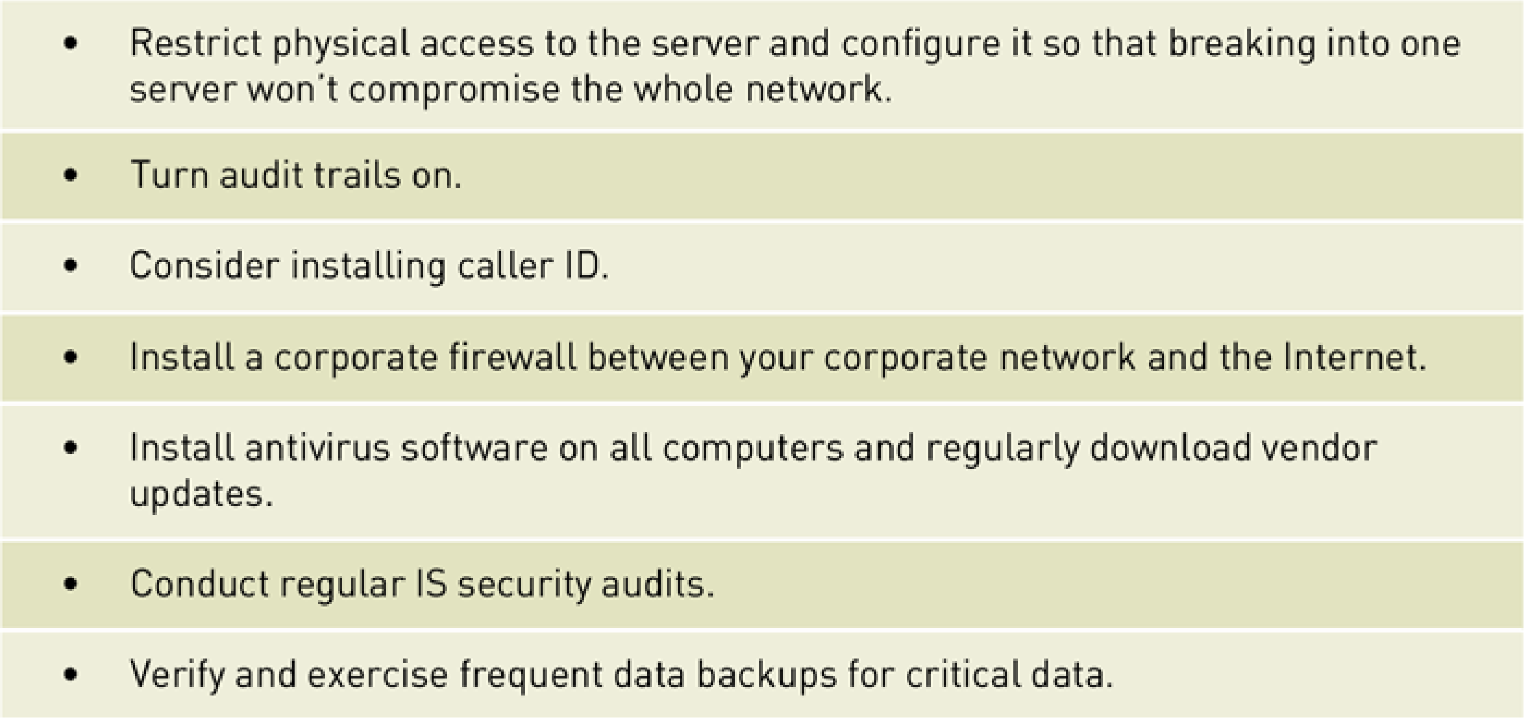
Preventing Computer-Related Crime (continued)



- Install strong user authentication and encryption capabilities on your firewall.
- Install the latest security patches, which are often available at the vendor's Internet site.
- Disable guest accounts and null user accounts that let intruders access the network without a password.
- Do not provide overfriendly login procedures for remote users (e.g., an organization that used the word *welcome* on their initial logon screen found they had difficulty prosecuting a hacker).
- Give an application (e-mail, file transfer protocol, and domain name server) its own dedicated server.

Table 9.9: How to Protect Your Corporate Data from Hackers

Preventing Computer-Related Crime (continued)



- Restrict physical access to the server and configure it so that breaking into one server won't compromise the whole network.
- Turn audit trails on.
- Consider installing caller ID.
- Install a corporate firewall between your corporate network and the Internet.
- Install antivirus software on all computers and regularly download vendor updates.
- Conduct regular IS security audits.
- Verify and exercise frequent data backups for critical data.

Table 9.9: How to Protect Your Corporate Data from Hackers (continued)

Preventing Computer-Related Crime (continued)

- **Intrusion detection system (IDS):** software that monitors system and network resources and notifies network security personnel when it senses a possible intrusion
- **Managed security service provider (MSSP):** an organization that monitors, manages, and maintains network security hardware and software for its client companies
- Internet laws for libel and protection of decency

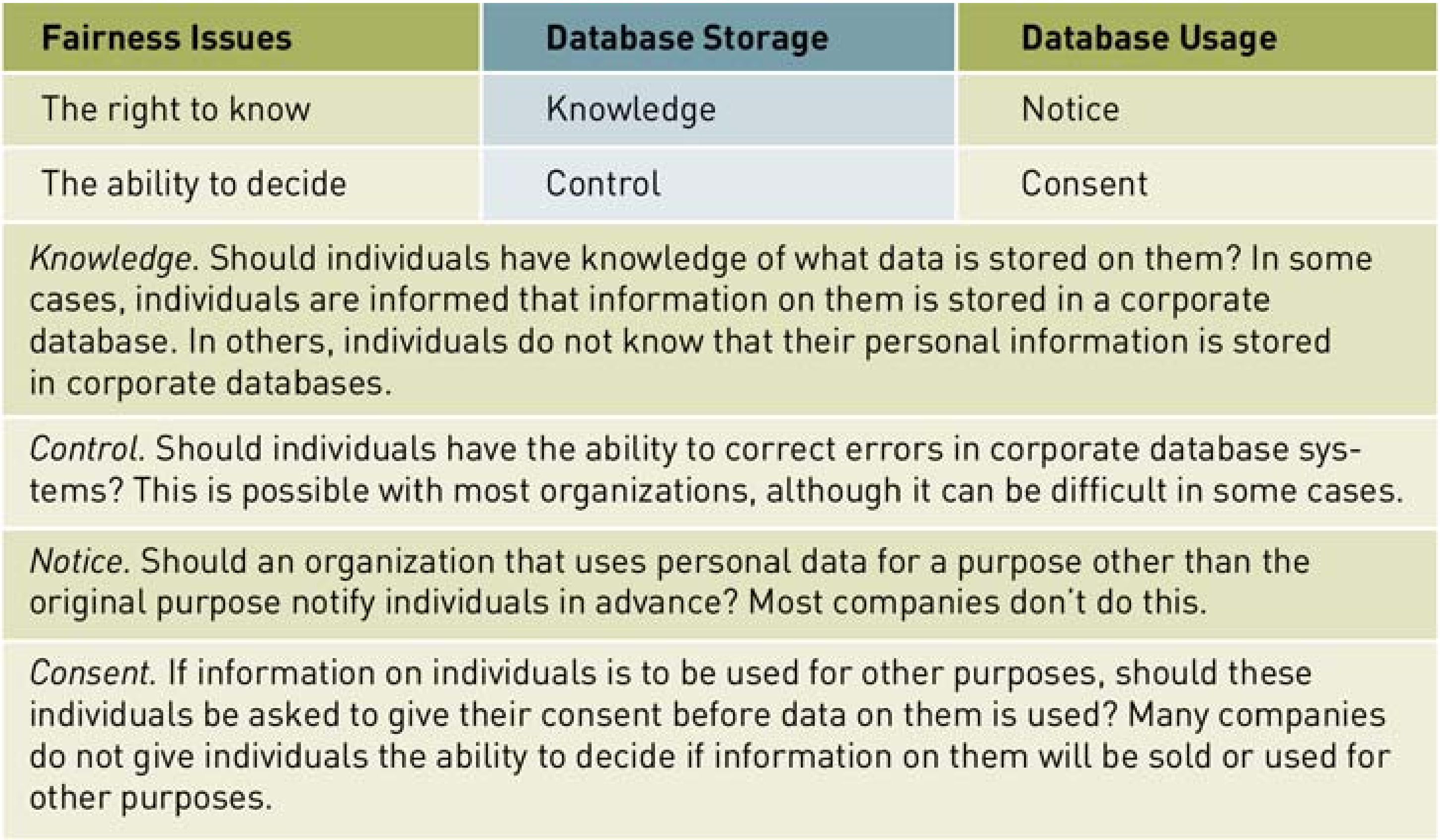
Preventing Crime on the Internet

- Develop effective Internet usage and security policies
- Use a stand-alone firewall with network monitoring capabilities
- Deploy intrusion detection systems, monitor them, and follow up on their alarms
- Monitor managers and employees
- Use Internet security specialists to perform audits

Privacy Issues

- With information systems, privacy deals with the collection and use or misuse of data
- Privacy and the federal government
- Privacy at work
- E-mail privacy
- Privacy and the Internet

Fairness in Information Use



Fairness Issues	Database Storage	Database Usage
The right to know	Knowledge	Notice
The ability to decide	Control	Consent

Knowledge. Should individuals have knowledge of what data is stored on them? In some cases, individuals are informed that information on them is stored in a corporate database. In others, individuals do not know that their personal information is stored in corporate databases.

Control. Should individuals have the ability to correct errors in corporate database systems? This is possible with most organizations, although it can be difficult in some cases.

Notice. Should an organization that uses personal data for a purpose other than the original purpose notify individuals in advance? Most companies don't do this.

Consent. If information on individuals is to be used for other purposes, should these individuals be asked to give their consent before data on them is used? Many companies do not give individuals the ability to decide if information on them will be sold or used for other purposes.

Table 9.10: The Right to Know and the Ability to Decide

Federal Privacy Laws and Regulations

- The Privacy Act of 1974
- Gramm-Leach-Bliley Act
- USA Patriot Act
- Other federal privacy laws

State Privacy Laws and Regulations

- State legislatures have been considering and passing privacy legislation that is far-reaching and potentially more burdensome to business than existing federal legislation
- State-by-state and county-by-county exceptions to the federal law complicate financial record keeping and data sharing

Corporate Privacy Policies

- Should address a customer’s knowledge, control, notice, and consent over the storage and use of information
- May cover who has access to private data and when it may be used
- A good database design practice is to assign a single unique identifier to each customer

Individual Efforts to Protect Privacy

- Find out what is stored about you in existing databases
- Be careful when you share information about yourself
- Be proactive to protect your privacy
- When purchasing anything from a Web site, make sure that you safeguard your credit card numbers, passwords, and personal information

Ethical Issues in Information Systems

- “Old contract” of business: the only responsibility of business is to its stockholders and owners
- “Social contract” of business: businesses are responsible to society

The AITP Code of Ethics

- Obligation to management
- Obligation to fellow AITP members
- Obligation to society
- Obligation to college or university
- Obligation to the employer
- Obligation to country

The ACM Code of Professional Conduct

- Strive to achieve the highest quality, effectiveness, and dignity in both the process and products of professional work
- Acquire and maintain professional competence
- Know and respect existing laws pertaining to professional work
- Accept and provide appropriate professional review
- Give comprehensive and thorough evaluations of computer systems and their impact, including analysis of possible risks

The ACM Code of Professional Conduct (continued)

- Honor contracts, agreements, and assigned responsibilities
- Improve public understanding of computing and its consequences
- Access computing and communication resources only when authorized to do so

Summary

- Preventing computer-related waste and mistakes requires establishing, implementing, monitoring, and reviewing policies and procedures
- Criminals need two capabilities to commit most computer crimes: knowing how to gain access to the computer system and knowing how to manipulate the system to produce the desired result

Summary (continued)

- Categories of crimes in which the computer is the object of crime: illegal access and use, data alteration and destruction, information and equipment theft, software and Internet piracy, computer-related scams, and international computer crime
- Intrusion detection system (IDS): software that monitors system and network resources and notifies network security personnel when it senses a possible intrusion

Summary (continued)

- With information systems, privacy deals with the collection and use or misuse of data
- “Old contract” of business: the only responsibility of business is to its stockholders and owners
- “Social contract” of business: businesses are responsible to society