Fundamentals of Information Systems, Fifth Edition

Chapter 9
The Personal and Social Impact of Computers
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
  – Discuss the principles and limits of an individual’s right to privacy
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
Principles and Learning Objectives (continued)

• Jobs, equipment, and working conditions must be designed to avoid negative health effects
  – List the important effects of computers on the work environment.
  – Identify specific actions that must be taken to ensure the health and safety of employees
Principles and Learning Objectives (continued)

• Practitioners in many professions subscribe to a code of ethics that states the principles and core values that are essential to their work
  – Outline criteria for the ethical use of information systems
Computer Waste and Mistakes

• Computer waste
  – 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 old software and even complete computer systems when they still have value
- Building and maintaining complex systems that are never used to their fullest extent
- Using corporate time and technology for personal use
- Spam
Computer-Related Mistakes

• Causes:
  – Failure by users to follow proper procedures
  – Unclear expectations and a lack of feedback
  – Program development that contains errors
  – Incorrect data entry by data-entry clerk
Preventing Computer-Related Waste and Mistakes

• Preventing waste and mistakes involves:
  – Establishing policies and procedures
  – Implementing policies and procedures
  – Monitoring policies and procedures
  – Reviewing policies and procedures
Implementing Policies and Procedures

• Establish policies and procedures regarding efficient acquisition, use, and disposal of systems and devices
• Training programs for individuals and workgroups
• Manuals and documents on how computer systems are to be maintained and used
• Approval of certain systems and applications to ensure compatibility and cost-effectiveness
Implementing Policies and Procedures

• Policies often focus on:
  – Implementation of source data automation and the use of data editing to ensure data accuracy and completeness
  – Assignment of clear responsibility for data accuracy within each information system

• Training
  – Key aspect of implementation
Monitoring Policies and Procedures

• Monitor routine practices and take corrective action if necessary
• Implement internal audits to measure actual results against established goals
Reviewing Policies and Procedures

• During review, people should ask the following questions:
  – Do current policies cover existing practices adequately?
  – Does the organization plan any new activities in the future?
  – Are contingencies and disasters covered?
Computer Crime

• Financial fraud, followed by virus attacks
  – The leading cause of financial loss from computer incidents
• Average annual loss from computer incidents is $350,424
• Computer crime is now global
The Computer as a Tool to Commit Crime

• Social engineering
  – Using social skills to get computer users to provide information to access an information system or its data

• Dumpster diving
  – Going through the trash cans of an organization to find confidential information, including information needed to access an information system
Cyberterrorism

- Cyberterrorist
  - Intimidates or coerces a government to advance his or her political or social objectives by launching computer-based attacks against computers, networks, and the information stored on them
Identity Theft

• Imposter obtains key pieces of personal identification information in order to impersonate someone else

• Consumers can help protect themselves by:
  – Regularly checking their credit reports with major credit bureaus
  – Following up with creditors if their bills do not arrive on time
  – Not revealing any personal information in response to unsolicited e-mail or phone calls
Internet Gambling

• Size of the online gambling market is not known
  – Estimate is that $10–20 billion is wagered on online poker alone each year

• Revenues generated by Internet gambling
  – Represent a major untapped source of income for the state and federal governments
The Computer as the Object of Crime

• Crimes fall into several categories such as:
  – Illegal access and use
  – Data alteration and destruction
  – Information and equipment theft
  – Software and Internet piracy
  – Computer-related scams
  – International computer crime
Illegal Access and Use

• Hacker
  – Learns about and uses computer systems

• Criminal hacker (cracker)
  – Gains unauthorized use or illegal access to computer systems

• Script bunnies
  – Automate the job of crackers

• Insider
  – Employee who compromises corporate systems
Illegal Access and Use (continued)

• **Virus**
  – Computer program file capable of attaching to disks or other files and replicating itself repeatedly

• **Worm**
  – Parasitic computer programs that replicate but do not infect other computer program files

• **Trojan horse**
  – Disguises itself as a useful application or game and purposefully does something the user does not expect
Using Antivirus Programs

• Antivirus program
  – Runs in the background to protect your computer from dangers lurking on the Internet and other possible sources of infected files

• Tips on using antivirus software:
  – Run and update antivirus software often
  – Scan all removable media before use
  – Install software only from a sealed package or secure, well-known Web site
  – Follow careful downloading practices
  – If you detect a virus, take immediate action
Spyware

• Software installed on a personal computer to:
  – Intercept or take partial control over the user’s interaction with the computer without knowledge or permission of the user
Information and Equipment Theft

• Data and information
  – Assets or goods that can also be stolen

• Password sniffer
  – Small program hidden in a network or a computer system that records identification numbers and passwords
Safe Disposal of Personal Computers

- Deleting files and emptying the Recycle Bin does not make it impossible for determined individuals to view the data.
- To make data unrecoverable use disk-wiping software utilities that overwrite all sectors of your disk drive.
Patent and Copyright Violations

• Software piracy
  – The act of unauthorized copying or distribution of copyrighted software
  – Penalties can be severe

• Patent infringement
  – Occurs when someone makes unauthorized use of another’s patent
Computer-Related Scams

• To avoid becoming a scam victim:
  – Do not agree to anything in a high-pressure meeting or seminar
  – Do not judge a company based on appearances
  – Avoid any plan that pays commissions simply for recruiting additional distributors
  – Do your homework
International Computer Crime

• Computer crime is an international issue
• Software industry loses about $11 to $12 billion in revenue to software piracy annually
Preventing Computer-Related Crime

- All states have passed computer crime legislation
- Some believe that these laws are not effective because:
  - Companies do not always actively detect and pursue computer crime
  - Security is inadequate
  - Convicted criminals are not severely punished
Crime Prevention by State and Federal Agencies

- State and federal agencies have begun aggressive attacks on computer criminals
- Computer Fraud and Abuse Act, 1986
  - Mandates punishment based on the victim’s dollar loss
- Computer Emergency Response Team (CERT)
  - Responds to network security breaches and monitors systems for emerging threats
Crime Prevention by Corporations

• Encryption
  – The process of converting an original electronic message into a form that can be understood only by the intended recipients

• To protect your computer from criminal hackers:
  – Install strong user authentication and encryption capabilities on your firewall
  – Install the latest security patches
  – Disable guest accounts and null user accounts
  – Turn audit trails on
Using Intrusion Detection Software

• Monitors system and network resources and notifies network security personnel when it senses a possible intrusion
• Can provide false alarms that result in wasted effort
Security Dashboard

• Employed to:
  – Provide a comprehensive display on a single computer screen of all the vital data related to an organization’s security defenses

• Data comes from a variety of sources including:
  – Firewalls
  – Applications
  – Servers
  – Other software and hardware devices
Using Managed Security Service Providers (MSSPs)

- MSSPs
  - Monitors, manages, and maintains network security for both hardware and software
  - Provide vulnerability scanning and Web blocking/filtering capabilities
Filtering and Classifying Internet Content

• Filtering software
  – Screens Internet content
  – Used by companies to prevent employees from visiting nonwork-related Web sites

• Internet Content Rating Association (ICRA)
  – Goals are to protect children from potentially harmful material, while also safeguarding free speech on the Internet
Internet Libel Concerns

• Companies should be aware that:
  – Publishing Internet content to the world can subject them to different countries’ laws

• Geolocation tools
  – Match user’s IP address with outside information to determine the actual geographic location of the online user

• Individuals
  – Must be careful what they post on the Internet to avoid libel charges
Preventing Crime on the Internet

- Develop effective Internet usage and security policies for all employees
- Use a stand-alone firewall (hardware and software) with network monitoring capabilities
- Deploy intrusion detection systems, monitor them, and follow up on their alarms
Preventing Crime on the Internet (continued)

- Monitor managers and employees to make sure that they are using the Internet for business purposes
- Use Internet security specialists to perform audits of all Internet and network activities
Privacy Issues

• Issue of privacy
  – Deals with this right to be left alone or to be withdrawn from public view

• More data and information are produced and used today than ever before
  – “Who owns this information and knowledge?”
Privacy and the Federal Government

• U.S. federal government
  – Perhaps the largest collector of data

• European Union
  – Has a data-protection directive that requires firms transporting data across national boundaries to have certain privacy procedures in place
Privacy at Work

• There is conflict between rights of workers who want their privacy and the interests of companies that demand to know more about their employees

• Nearly one-third of companies have fired an employee for violating corporate e-mail policies
E-Mail Privacy

• Federal law
  – Permits employers to monitor e-mail sent and received by employees
• E-mail messages that have been erased from hard disks can be retrieved and used in lawsuits
• Use of e-mail among public officials might violate “open meeting” laws
Instant Messaging Privacy

- Using instant messaging (IM) to send and receive messages, files, and images introduces the same privacy issues associated with e-mail
- Do not send personal or private IMs at work
Privacy and Personal Sensing Devices

• RFID tags
  – Essentially microchips with antenna, are embedded in many of the products we buy
  – Generate radio transmissions that, if appropriate measures are not taken, can lead to potential privacy concerns
Privacy and the Internet

- Platform for Privacy Preferences (P3P)
  - Screening technology that shields users from Web sites that do not provide the level of privacy protection they desire

- Children’s Online Privacy Protection Act (COPPA), 1998
  - Require privacy policies and parental consent
Fairness in Information Use

• Laws passed regarding a person’s right to privacy
  – The Privacy Act of 1974
  – Gramm-Leach-Bliley Act
  – USA Patriot Act
  – Other Federal Privacy Laws
Fairness in Information Use (continued)

<table>
<thead>
<tr>
<th>Fairness Issues</th>
<th>Database Storage</th>
<th>Database Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to know</td>
<td>Knowledge</td>
<td>Notice</td>
</tr>
<tr>
<td>The ability to decide</td>
<td>Control</td>
<td>Consent</td>
</tr>
</tbody>
</table>

**Knowledge.** Should people know what data is stored about them? In some cases, people are informed that information about them is stored in a corporate database. In others, they do not know that their personal information is stored in corporate databases.

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

---

**Table 9.2**

| The Right to Know and the Ability to Decide Federal Privacy Laws and Regulations |
Corporate Privacy Policies

• Invasions of privacy
  – Can hurt business, turn away customers, and dramatically reduce revenues and profits

• Multinational companies
  – Face an extremely difficult challenge in implementing data collection and dissemination processes and policies
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
The Work Environment

• Computer technology and information systems
  – Have opened up numerous avenues to professionals and nonprofessionals
• Despite increases in productivity and efficiency computers and information systems can raise other concerns
Health Concerns

• Working with computers
  – Can cause occupational stress

• Training and counseling
  – Can often help the employee and deter problems

• Carpal tunnel syndrome (CTS)
  – Aggravation of the pathway for the nerves that travel through the wrist (carpal tunnel)
Avoiding Health and Environmental Problems

- Many computer-related health problems
  - Are caused by a poorly designed work environment
- Ergonomics
  - Science of designing machines, products, and systems to maximize the safety, comfort, and efficiency of the people who use them
Ethical Issues in Information Systems

• Code of ethics
  – States the principles and core values that are essential to a set of people and thus governs their behavior
Summary

• Computer waste
  – Inappropriate use of computer technology and resources in both the public and private sectors
• Some crimes use computers as tools
• Computer crimes target computer systems and include:
  – Illegal access to computer systems by criminal hackers
  – Alteration and destruction of data and programs by viruses
  – Theft of computer resources
Summary (continued)

- Because of increased computer use greater emphasis is placed on the prevention and detection of computer crime
- Although most companies use data files for legitimate, justifiable purposes opportunities for invasion of privacy abound
- A business should:
  - Develop a clear and thorough policy about privacy rights for customers, including database access
Summary (continued)

• Computers have:
  – Changed the makeup of the workforce and even eliminated some jobs
  – Expanded and enriched employment opportunities in many ways

• Ethics
  – Determine generally accepted and discouraged activities within a company and society at large