MIS

CHAPTER 4

PERSONAL, LEGAL, ETHICAL, AND ORGANIZATIONAL ISSUES OF INFORMATION SYSTEMS

Hossein BIDGOLI

Phishing

Email that bites

Paying for Privacy

Pirates

learning outcomes

LO1 Describe information technologies that could be used in computer crimes.

LO2 Review privacy issues and methods for improving privacy of information.

LO3 Explain the effects of e-mail, data collection, and censorship on privacy.

LO4 Discuss ethical issues of information technology.

LO5 Describe intellectual property principles and infringement issues.

learning outcomes (cont'd.)

LO6 **Explain information system issues affecting organizations, including the digital divide, electronic publishing, and effects on the workplace and employees' health.**

Risks Associated with Information Technologies

- Misuses of information technology
  - Invade users' privacy
  - Commit computer crimes

Cookies

- **Cookies**
  - Small text files with a unique ID tag
  - Embedded in a Web browser
  - Saved on the user's hard drive
- Can be useful or intrusive
- Many users disable cookies
  - By installing a cookie manager
  - Or using Web browser options

Spyware and Adware

- **Spyware**
  - Software that secretly gathers information about users while they browse the Web
  - Can be used maliciously
- Install antivirus or antispyware software
- **Adware**
  - Form of spyware
  - Collects information about the user to display advertisements in the Web browser

Phishing

- **Phishing**
  - Sending fraudulent e-mails that seem to come from legitimate sources
- Direct e-mail recipients to false Web sites
  - To capture private information

Keyloggers, Sniffing and Spoofing

- **Keyloggers**
  - Some antivirus and antispyware programs protect against software keyloggers
- **Sniffing**
  - Capturing and recording network traffic
  - Often used by hackers to intercept information
- **Spoofing**
  - Attempt to gain access to a network by posing as an authorized user to find sensitive information

Computer Crime and Fraud

- Computer fraud
  - Unauthorized use of computer data for personal gain
- Social networking sites
  - Used for committing computer crime
- Examples
  - Denial-of-service attacks
  - Identity theft
  - Software piracy
  - Distributing child pornography
  - E-mail spamming

Computer Crime and Fraud (cont'd.)

- Writing or spreading viruses, worms, Trojan programs, and other malicious code
- Stealing files
- Changing computer records
- Virus hoaxes
- Sabotage

Computer Crime – Unauthorized Access

Unauthorized Access
A person gaining entry to a computer system for which they have no authority to use such access

THIS IS A COMPUTER CRIME!

82% come from inside the organization (employees)

Privacy Issues

- Concerns about privacy in the workplace
- Misuse and abuse of information gathered by: ….
- Defining privacy is difficult
- Number of databases increasing rapidly
  - Direct marketing companies major user of this information
- U.S. government began linking large databases to find information
- **Acceptable use policies**

E-mail

- Presents some serious privacy issues
- **Spamming**
  - Unsolicited e-mail sent for advertising purpose
  - Sent in bulk by using automated mailing software
- Ease of access
  - People should assume that others could have access to their messages
  - Any e-mails sent on company-owned computers are the property of the organization

E-mail and Spam Statistics

Table 4.1

E-mail and Spam Statistics

1.3 billion	Number of e-mail users worldwide
210 billion	Number of e-mails sent per day
70%	Percentage of e-mails that are spam
53.8 trillion	Number of spam e-mails sent in 2008

Ethical Issues of Information Technologies

- Ethics and ethical decision making
  - Moral guidelines people or organizations follow in dealing with others
  - More difficult to determine than legal cersus illegal

Exhibit 4.1 *Ethical versus legal grid*

	Legal	Illegal
Ethical	I	II
Unethical	III	IV

Censorship

- Who decides what should be on the Internet?
- Whether or not something can be censored depends in part on who is doing the censoring
- Parents are concerned about what their children are exposed to
  - Pornography, violence, and adult language
- Mistaken or mistyped URLs
- Search terms

Intellectual Property

- **Intellectual property**
  - Protections that involve copyrights, trademarks, trade secrets, and patents for “creations of the mind” developed by people or businesses
- Industrial property
  - Inventions, trademarks, logos, industrial designs
- Copyrighted material
- **Cybersquatting**
  - Registering, selling, or using a domain name to profit from someone else’s trademark

The Impact of Information Technology in the Workplace

- New jobs
- Telecommuting and virtual work
- Job deskilling
- Job upgrading
- One skilled worker might be capable doing the job of several workers
- Virtual organizations
- Green Computing
  - promotes a sustainable environment and consumes the least amount of energy

Advantages and Disadvantages of Telecommuting

Benefit	Potential drawback
Ability to care for small children or elderly parents and spend more time with family	Possibility of becoming a workaholic (no hard boundaries between "at work" and "at home").
Having fewer restrictions on clothing for work and saving the expense of workwear	Not having a regulated work routine
No commute, so distance and time factors are reduced as well as the effects of car emissions on air quality	Less interaction with co-workers
Ability to work in more pleasant surroundings	No separation between work and home life
Increased productivity	Potential legal issues about workers' injuries
Decreased neighborhood crime because of more people being home during the day	Family interruptions and household distractions
Home environment might be easier for employees with disabilities	Lack of necessary supplies or equipment
Reduced costs for office space and utilities	Might create a two-tiered workforce—telecommuters and on-site workers—that affects promotions and raises
Reduced employee turnover and absenteeism	Not all jobs are suitable for telecommuting
Ability to find and hire people with special skills, regardless of where they're located	
Work with fewer interruptions from co-workers	

Summary

- Information technologies
  - Affect privacy
  - Can be used for computer crimes
  - Privacy issues
  - E-mail
  - Censorship
- Organizational issues
  - Digital divide
  - Workplace impacts
  - Health impact

©2011 Course Technology, a part of Cengage Learning

Consider the following situations:

Situation A: Suppose you are buying a condo and you know that at least one other party is bidding against you. While agonizing over your best strategy, you stop at a local Starbucks. As you sip your latte, you overhear a conversation at the table next to yours. Three people are talking loudly enough that it is difficult to ignore them, and you soon realize that they are the real estate agent and the couple who is competing for the condo you want. They are preparing their offer. Should you listen to their conversation? If you do, do you use the information you hear to your advantage?

©2011 Course Technology, a part of Cengage Learning

Situation B: Consider the same situation from a different perspective—instead of overhearing the conversation, suppose you receive that same information in an email. Perhaps an administrative assistant at the agent's office confuses you and the other customer and mistakenly sends you the terms of the other party's offer. Do you read that email? If so, do you use the information that you read to your advantage?

©2011 Course Technology, a part of Cengage Learning

1. Answer the questions in situations A and B. Do your answers differ? Does the medium by which the information is obtained make a difference? Is it easier to avoid reading an email than it is to avoid hearing a conversation? If so, does that difference matter?

©2011 Course Technology, a part of Cengage Learning

Situation C: Suppose that you sell computer software. In the midst of a sensitive price negotiation, your customer accidentally sends you an internal email that contains the maximum amount that the customer can pay for your software. Do you read that email? Do you use that information to guide your negotiating strategy? If your customer discovers that the email may have reached you and asks, "Did you read my email?" how do you answer?

©2011 Course Technology, a part of Cengage Learning

2. Answer the questions in situations B and C. Do your answers differ? In situation B, the information is for your personal gain; in C, the information is for both your personal and your organization's gain. Does this difference matter? How do you respond when asked if you have read the email?

©2011 Course Technology, a part of Cengage Learning

Situation D: Suppose a friend mistakenly sends you an email that contains sensitive personal medical data. Further, suppose you read the email before you know what you're reading and you're embarrassed to learn something very personal that truly is none of your business. Your friend asks you, "Did you read that email?" How do you respond?

©2011 Course Technology, a part of Cengage Learning

3. Answer the questions in situations C and D. Do your answers differ? Would you lie in one case and not in the other? Why or why not?

©2011 Course Technology, a part of Cengage Learning

Situation E: Finally, suppose that you work as a network administrator and your position allows you unrestricted access to the mailing lists for your company. Assume that you have the skill to insert your email address into any company mailing list without anyone knowing about it. You insert your address into several lists and, consequently, begin to receive confidential email that no one intended for you to see. One of those emails indicates that your best friend's department is about to be eliminated and all of its personnel fired. Do you forewarn your friend?

©2011 Course Technology, a part of Cengage Learning

4. Answer the questions in situation E. What is the essential difference between situations A through D and situation E? Suppose you had to justify your behavior in situation E. How would you argue? Do you believe your own argument?

©2011 Course Technology, a part of Cengage Learning

5. In situations A through D, if you access the information you have done nothing illegal. You were the passive recipient. Even for item E, although you undoubtedly violated your company's employment policies, you most likely did not violate the law. So, for this discussion, assume that all of these actions are legal.

a. What is the difference between legal and ethical? Look up each term in a dictionary and explain how they differ.

b. Make the argument that business is competitive, and that if something is legal, then it is acceptable to do it if it helps to further your goals.

c. Make the argument that it is never appropriate to do something unethical.

©2011 Course Technology, a part of Cengage Learning

Phishing

- **Phishing**
  - Sending fraudulent e-mails that seem to come from legitimate sources
- Direct e-mail recipients to false Web sites
  - To capture private information

©2011 Course Technology, a part of Cengage Learning