**Chapter 13 :** Security and Ethical Challenges

**True / False Questions**

1. As a manager or business professional you should manage your work activities and those of others to minimize the detrimental effects of e-business systems and optimize their beneficial effects.

True False

2. Scheduling work breaks and limiting exposure to computer monitors are examples of ethical behavior by organizations.

True False

3. Many companies and organizations have established guidelines for ethical conduct, but very few specify that company computer workstations and networks are company resources to be used for work-related uses only.

True False

4. Cyber crime is becoming one of the Net's growth businesses.

True False

5. According to the text case, it is reasonably easy for law enforcement to catch "bad guys" on the Internet.

True False

6. Electronic breaking and entering means getting access to a computer system, reading some files, but neither stealing nor damaging anything.

True False

7. A malicious applet is an instruction in a computer program that triggers a malicious act.

True False

8. A sniffer is a program that covertly searches individual packets of data as they pass through the Internet, capturing passwords or content.

True False

9. A hacker is a person who maintains knowledge of the vulnerabilities and exploits he or she finds for private advantage, and does not reveal them either to the general public or to the manufacturer for correction.

True False

10. Most companies don't reveal that they have been targets or victims of computer crime.

True False

11. Moonlighting is an Internet abuse where an employee is paid by outsiders for allowing them to use the company's Internet services for free.

True False

12. Using office resources, such as networks and computers, to search for side jobs is generally not considered workplace Internet abuse.

True False

13. According to one survey, 90 percent of U.S. workers admit to surfing recreational sites during office hours.

True False

14. According to the text case, about two-thirds of the companies surveyed monitor their Internet connections, but only two states require informing employees that they do so.

True False

15. The music industry reports that illegal downloading of music and videos is a growing problem.

True False

16. A virus is a distinct program that can run unaided.

True False

17. Spyware is annoying, but generally no threat to your privacy.

True False

18. Confidential e-mail messages are seldom monitored, although other business communication routinely is.

True False

19. In the United States, opt-out is the default position, whereas in Europe consumers must opt-in or their personal information cannot be used.

True False

20. The use of information technologies is causing a significant reduction in some types of job opportunities.

True False

21. Computer monitoring has been criticized as unethical because no one is overseeing the person who monitors the workers.

True False

 22. Computer monitoring has been criticized as an invasion of employee privacy because it uses video as well as keystroke surveillance.

True False

23. Lawsuits by monitored workers against employers are increasing.

True False

24. The widespread use of personal computers and the Internet has dramatically improved the development of people-oriented and personalized information systems.

True False

 25. People who sit at PC workstations or visual display terminals in fast-paced, repetitive-keystroke jobs can suffer from a variety of health problems, known collectively as computer trauma disorders (CTDs).

True False

26. According to the text, the need for security management is being driven by the increasing threat of cybercrimes and by the growing use of the Internet to link companies with partners and customers.

True False

27. The most widely used encryption method uses a pair of public and private keys unique to each individual.

 True False

 28. Firewall software has become essential for individuals connecting to the Internet with DSL or cable modems because of their faster download speeds.

True False

 29. According to the text case, monitoring employees use of email and the Internet has become commonplace.

True False

30. These days, corporate antivirus protection is a centralized function of information technology.

True False

31. Security suites integrate virus protection with firewalls, Web security, and encrypted e-mail.

True False

 32. In some systems, the password to read the contents of a file is different from that required to write to a file (change its contents).

True False

 33. Security monitors can control the use of the hardware, software, and data resources of a computer system.

True False

 34. Biometric control devices use special-purpose sensors to measure and digitize a biometric profile of an individual's fingerprints, voice, or other physical trait.

True False

35. IS controls are needed to ensure the proper entry of data into a business system and thus avoid the gigabytes in, gigabytes out (GIGO) syndrome.

True False

36. IT security management should be periodically examined or audited by a company's internal auditing staff or auditors from professional accounting firms.

True False

**Multiple Choice Questions**

37. As a business professional, you have a responsibility to promote ethical uses of information technology in the workplace. This responsibility includes:

1. Performing your role as a vital business resource by participating on every development team
2. Using the Internet only during breaks and after-work hours
3. Performing your role as a vital human resource in the business systems you help develop and use in your organization
4. Documenting all employee electronic mail usage and Internet searches

38. According to the text, information technology has caused ethical controversy in all of the following basic categories of ethical business issues, except:

1. Intellectual property rights
2. Whistle blowing
3. Customer and employee privacy
4. Workplace safety

39. According to the text, information technology has caused ethical controversy in which of the following basic categories of ethical business issues?

1. Comparable worth
2. Whistle blowing
3. Workplace safety
4. Employee conflicts of interest

40. According to the text, which are the four basic categories of ethical business issues where information technology has caused ethical controversy?

1. Intellectual property rights, customer and employee privacy, security of company information, and workplace safety
2. Executive salaries, affirmative action, whistle blowing, and advertising content
3. Product pricing, shareholder interests, inappropriate gifts, divestment
4. Comparable worth, sexual harassment, employee conflicts of interest, product safety

41. When managers apply the \_\_\_\_\_\_\_\_\_\_\_\_\_ theory of ethical decision making, they believe that companies have ethical responsibilities to all members of society.

1. social contract
2. stakeholder
3. stockholder
4. Midas

42. When managers apply the \_\_\_\_\_\_\_\_\_\_\_\_\_ theory of ethical decision making, they believe that managers have an ethical responsibility to manage a firm for the benefit of all individuals and groups that have a claim on a company.

1. social contract
2. stakeholder
3. stockholder
4. Midas

43. When managers apply the \_\_\_\_\_\_\_\_\_\_\_\_\_ theory of ethical decision making, they believe their only responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices.

1. social contract
2. stakeholder
3. stockholder
4. Midas

44. The social contract theory maintains that:

1. Companies have ethical responsibilities to all members of society, which allow corporations to exist based on a social contract
2. Managers are agents of the organization's owners, and their only ethical responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices
3. Managers have an ethical responsibility to manage a firm for the benefit of all individuals and groups that have a claim on a company
4. Managers are agents of the customer, and their only ethical responsibility is to increase the service of the business, without violating the law or engaging in fraudulent practices

45. The stockholder theory maintains that:

1. Companies have ethical responsibilities to all members of society, which allow corporations to exist based on a social contract
2. Managers are agents of the organization's owners, and their only ethical responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices
3. Managers have an ethical responsibility to manage a firm for the benefit of all individuals and groups that have a claim on a company
4. Managers are agents of the customer, and their only ethical responsibility is to increase the service of the business, without violating the law or engaging in fraudulent practices

46. The stakeholder theory maintains that:

1. Companies have ethical responsibilities to all members of society, which allow corporations to exist based on a social contract
2. Managers are agents of the organization's owners, and their only ethical responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices
3. Managers have an ethical responsibility to manage a firm for the benefit of all individuals and groups that have a claim on a company
4. Managers are agents of the customer, and their only ethical responsibility is to increase the service of the business, without violating the law or engaging in fraudulent practices

47. According to the text, all the following are examples of ethical behavior by organizations, except:

1. Scheduling work breaks
2. Stockholder theory
3. Limiting exposure to computer monitors
4. Preventing hand or eye injuries

48. One of the major principles of technology ethics is that the good achieved by the technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk. This principle is:

1. Informed consent
2. Justice
3. Minimized risk
4. Proportionality

49. Which of the following best describes the ethical principle of informed consent?

1. The good achieved by technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk
2. Those affected by technology should understand and accept the risks
3. The benefits and burdens of technology should be distributed fairly. Those who benefit should bear their fair share of the risks, and those who do not benefit should not suffer a significant increase in risk
4. Even if judged acceptable by the other guidelines, the technology must be implemented so as to avoid all unnecessary risks

50. One of the major principles of technology ethics is that even if judged acceptable by the other three guidelines, the technology must be implemented so as to avoid all unnecessary risk. This principle is:

1. Informed consent
2. Justice
3. Minimized risk
4. Proportionality

51. All of the following are AITP standards of professional conduct related to a person's obligation to society except:

1. Protect the privacy and confidentiality of all information entrusted to me
2. To the best of my ability, ensure that the products of my work are used in a socially responsible way
3. Never misrepresent or withhold information that is germane to a problem or a situation of public concern
4. Do not use knowledge of a confidential or personal nature in any unauthorized manner to achieve personal gain

52. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is/are the most commonly used security technology at large companies.

1. Intrusion-detection systems
2. Smart cards
3. Biometrics
4. Antivirus software

53. According to the text, all of the following statements are included in the definition of computer crime except:

1. Unauthorized modification of software, data, or network resources
2. Unauthorized release of information
3. Unauthorized copying of software
4. Unauthorized distribution of public domain software

54. According to the text, companies are protecting themselves from computer crime by using:

1. Antivirus software
2. Intrusion-detection systems
3. Biometrics
4. All of the choices are correct.

55. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ means getting access to a computer system, reading some files, but neither stealing nor damaging anything.

1. Electronic breaking and entering
2. Sniffing
3. Snooping
4. Dumpster diving

56. The text defines \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ as the obsessive use of computers, or the unauthorized access and use of networked computer systems.

1. hacking
2. cyber-slacking
3. cracking
4. resource theft

57. The text defines a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ as a person who maintains knowledge of the vulnerabilities he or she finds and exploits them for private advantage, not revealing them to either the general public or the manufacturer for correction.

1. hacker
2. cyber-slacking
3. cracker
4. resource theft

58. Hammering a Web site's equipment with too many requests for information, slowing performance or even crashing the site is called:

1. A logic bomb
2. Denial of service
3. A back door
4. Social engineering

59. Sifting through a company's garbage looking for information to help break into the company's computers; sometimes used in conjunction with social engineering is called:

1. Dumpster diving
2. Denial of service
3. A back door
4. A sniffer

60. Talking unsuspecting company employees out of valuable information such as passwords is called:

1. Sniffing
2. Denial of service
3. A back door
4. Social engineering

61. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is software that can guess passwords.

1. logic bomb
2. password cracker
3. back door
4. sniffer

62. One way hackers gain access to an individual's information is by faking an e-mail address or Web page to trick users into passing along critical information like credit card numbers. This is known as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. sniffing
2. hacking
3. phishing
4. spoofing

63. According to the text case, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ of people have stolen key information from work.

1. 10%
2. 20%
3. 70%
4. 80%

64. According to the text, companies can use \_\_\_\_\_\_\_\_\_\_ to attack the problem of unauthorized use of computer systems and networks, to monitor network traffic in order to reveal evidence of improper use.

1. sniffers
2. snoopers
3. zombies
4. password crackers

65. To use public domain software legally, a company:

1. Must purchase individual copies or a site license for a certain number of copies
2. Can examine a single copy of the software for 30 days and then purchase as many copies as needed
3. Can make as many copies as desired because the software is not copyrighted
4. None of the choices are correct.

66. Software that is not copyrighted is called:

1. Shareware
2. Open source
3. Public domain
4. None of the choices are correct.

67. All of the following are common ways for a computer virus to enter a computer system except:

1. E-mail and file attachments
2. Running antivirus programs
3. Downloaded copies of shareware
4. Borrowed copies of software

68. Which of the following statements about adware and spyware is true?

1. Protecting against this software usually requires the purchase and installation of programs designed to prevent the software from being downloaded and installed
2. Removal programs are 100% successful, although they are very expensive
3. Adware software removes spyware software from a user's computer
4. A user must approve the downloading of adware, even if tricked into doing so

69. Governments around the world are debating privacy issues and considering various forms of legislation. One area central to the privacy debate is opt-in versus opt-out. Those preferring the opt-in standard do so because this standard would:

1. Make privacy the default for consumers
2. Make privacy the default, if a consumer calls in to request no data sharing
3. Make sharing private information the default
4. It would match the existing policy of most Internet-based companies

70. Individuals have been mistakenly arrested and jailed, and others have been denied credit because of their physical profiles or personal data. These are often the result of:

1. Computer profiling and computer matching
2. Unauthorized opt-in
3. Censorship
4. Adware

71. Indiscriminate sending of unsolicited e-mail messages to many Internet users is called\_\_\_\_\_\_\_\_\_\_\_\_.

1. flaming
2. spamming
3. spoofing
4. spying

72. Sending extremely critical, derogatory, and often vulgar e-mail messages is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. flaming
2. spamming
3. spoofing
4. spying

73. Computer monitoring has been criticized as unethical because:

1. It only monitors the work being done
2. Nobody is overseeing the person doing the monitoring
3. It is outside human control
4. It monitors individuals, not just the job

74. Computer monitoring has been criticized as an invasion of employee privacy because:

1. Many times employees do not know they are being monitored
2. Employees know how the information is being used
3. It monitors the work being done
4. It is outside human control

75. Information technologies have caused a significant reduction in the following types of job opportunities, except:

1. Accounting
2. Control of machine tools
3. E-commerce directors
4. All the answers are jobs that have been reduced by information technologies

76. Lawsuits by monitored workers against employers are:

1. increasing
2. decreasing
3. staying the same
4. no longer permitted in any of the 50 states

77. Which of the following is not a health issue commonly related to the use of information technology in the workplace?

1. Damaged arm and neck muscles
2. Eyestrain
3. Job stress
4. Hearing loss

78. People who sit at PC workstations or visual display terminals in fast-paced, repetitive-keystroke jobs can suffer from a variety of health problems, known collectively as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Computer trauma disorders
2. Eyestrain
3. Carpal tunnel distress
4. Cumulative trauma disorders

79. Good ergonomic design considers tools, tasks, the workstation, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. the users
2. the environment
3. the software
4. previous injuries

80. The goal of ergonomics is to design:

1. Effective work environments that are conducive to fast-paced, repetitive jobs
2. Efficient work environments that are productive and promote high morale
3. Healthy work environments that are safe, comfortable, and pleasant for people to work in
4. Policies regarding work environment structures

81. The text describes a/an \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ as a "gatekeeper" system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks.

1. firewall
2. filtered portal
3. encoder
4. telecommunications line

82. What is the purpose of external firewalls?

1. To prevent users from accessing sensitive human resource or financial data
2. To limit access of intranet resources to specific users
3. To avoid creating security holes to back-end resources
4. To keep out unauthorized Internet users from intranet networks

83. Firewall software has become essential for individuals connecting to the Internet with DSL or cable modems:

1. Because of their faster download speeds
2. Because of their "always on" connection status
3. Because antivirus software is not made for these connections
4. All the choices are correct

84. Which of the following is not a method used to defend against denial of service attacks at "zombie" machines?

1. Set and enforce security policies
2. Monitor employee emails
3. Remind users not to open .exe mail attachments
4. Close unused ports

85. In 2000, hackers broke into hundreds of servers and planted Trojan horse .exe programs, which were then used to launch a barrage of service requests in a concerted attack at e-commerce websites, such as Yahoo! and eBay. This is an example of a distributed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attack.

1. acceptance of service
2. denial of service
3. zombie
4. Trojan virus

86. Which of the following is a method used to defend against denial of service attacks at the victim's website?

1. Create backup servers and network connections
2. Limit connections to each server
3. Install multiple intrusion-detection systems and multiple routers for incoming traffic to reduce choke points
4. All of the choices are correct.

87. Security monitors can control the use of all the following except:

1. Hardware
2. Software
3. External networks
4. Data resources

88. According to the text, backup files:

1. Are duplicate files of data or programs
2. Can be used to reconstruct the original files if they are destroyed
3. May be stored off-premises, sometimes in special storage vaults in remote locations
4. All of the choices are correct.

89. According to the text, GIGO stands for:

1. Generalized input, gross output
2. Gateway input, gateway output
3. Gigabytes in, gigabytes out
4. Garbage in, garbage out

90. An effective disaster recovery plan would include which of the following?

1. Arrangements with other companies for use of alternative facilities as a disaster recovery site.
2. A listing of what hardware, software, and facilities will be used.
3. A listing of which applications will be processed, and in what priority.
4. All of the choices are correct.