|  |
| --- |
| **Chapter 3** **COMPUTER CRIME, ETHICS, AND PRIVACY** |

# True-False Questions

1. There is *no* complete, generally accepted definition of cybercrime presently available.
2. The largest known cybercrime of record is the TRW Company Credit Data Case.
3. Most computer abuse that we have caught so far has been because of good accounting controls.
4. According to the chapter, a computer virus is an example of a type of cybercrime called “denial of service.”
5. Many types of cybercrime have other, more common names such as "vandalism" or "embezzlement."
6. In the United States, trafficking in passwords is immoral, but not illegal.
7. The U. S. Congress passed the first federal computer crime law in 1986 making it illegal to alter or destroy federal information.
8. No one really knows how much is lost each year as the result of cybercrime.
9. The absence of good statistics on cybercrime is partially explained by the fact that a large proportion of the cybercrime committed in private organizations is handled as an internal matter and thus is never publicly divulged.
10. One conclusion that we can draw about cybercrime is that it is growing.
11. We believe that most cybercrime is *not* discovered.
12. There were less than 200 documented cases of cybercrime at the time the textbook was written.
13. Automated accounting information systems are a particularly important potential target of cybercrime.
14. When organizations discover a cybercrime, the cost of auditing and investigating the loss often exceeds the actual monetary loss.
15. The TRW Company Credit Data Case is an example of “valuable information” cybercrime.
16. A paradoxical matter in the TRW Case was that the prosecution had trouble acquiring testimonies because the buyers as well as the sellers of the credit information were in technical violation of the law.
17. A conflict exists between providing bona fide AIS users easy access to computer resources and security objectives.
18. It is generally accepted that hackers are motivated only by greed.
19. Worm programs are viruses that insert themselves into computer systems and disrupt operations or files.
20. A computer virus may lie dormant in a system until software is copied and run on non‑licensed machines.
21. Lockout systems disconnect telephone connections if users fail to provide a correct password in a set number of tries.
22. Dial-back systems help control unauthorized access to computer systems.
23. According to a recent CSI survey, the most common problem encountered by the respondents is viruses.
24. One reason why computer crime is important to AISs is because, according to a Computer Security Institute survey, the average cost of a computer-abuse incident is about $500,000.
25. According to a KPMG survey, companies that stress the importance of business ethics tend to get about the same results as companies that do *not* stress its importance.
26. A “strong password” is a password that lasts a long time.
27. Fortunately, thwarting most forms of cybercrime does *not* require the support of top management.
28. Experts suggest that policies on computer abuse are ineffective, and therefore should *not* be used to help educate employees about computer abuse.
29. Most computer criminals are individuals of questionable background, little education, and no morals.
30. Watching for tell-tale signs may help detect computer crime.
31. Most computer criminals we have been fortunate enough to catch have had long, criminal backgrounds.
32. Forensic accountants are to accounting as detectives are to criminal justice.
33. Today’s accountants have no responsibility for designing or implementing control procedures that protect AISs from cybercrime and fraud.
34. Cybercrime is another name for computer fraud.

## **Multiple-Choice Questions**

1. According to the chapter, which of these statements is most accurate?

a) Almost all cybercrime is committed for personal gain

1. Very little cybercrime is committed for personal gain
2. Most cybercrime is just as easily described as “embezzlement”
3. We actually know very little about cybercrime
4. According to the chapter, which of these statements is most accurate?

a) Most cybercrime is performed as retaliation against employers

1. Very little cybercrime is committed for personal gain
2. Some cybercrime is performed simply to meet a challenge
3. We catch most computer abusers with good accounting controls
4. Which of these would be an example of “denial-of-service” computer abuse?

a) Computer virus

b) Salami technique

c) Trojan horse computer program

d) Embezzlement using computerized data

e) none of these

1. Which of these terms describes a computer program that remains dormant until triggered by some specific circumstance or date?

a) Trojan horse program

b) DDoS program

c) Logic bomb

d) Dial back system

1. Much of what has been termed cybercrime has merely involved the computer but probably would be more accurately classified as other types of crimes. A notable exception to this involves:

a) Raiding dormant bank accounts

1. Inventory misappropriation
2. Embezzlement
3. Theft of computer time
4. The process of changing data before, during, or after they are entered into a computer system is called:
5. Data diddling
6. Salami techinique
7. Logic bombs
8. Social engineering
9. This term describes the technique of stealing small amounts of money from a large number of accounts over time.

a) Salami technique

1. Buffet system
2. Baloney method
3. Dialing for dollars
4. This best explains why we have incomplete information on cybercrime.

a) Most companies handle abuse as an internal matter

1. Most newspapers no longer have any interest in reporting cybercrime
2. Documentation of abuses is usually poor
3. We believe that most cybercrime is not caught
4. At present, we think that cybercrime is:

a) Falling

1. Random
2. Rising
3. Flat
4. All of these are reasons why we think that cybercrime is rising *except*:

a) Some Internet web sites now instruct users how to perform certain types of computer abuse

1. More people now know how to use computers
2. Computer usage continues to grow
3. all of these are reasons
4. According to the chapter, which of these statements is most accurate?

a) Today, most computers are safe from computer abuse

1. Today, very few computers are completely safe from computer abuse
2. Today, “hacking” is no longer possible
3. Today, all of these statements are accurate
4. The TRW Credit Data Case is an example of:

a) The round‑off trick

1. An outsider ripping off a corporate computer
2. Valuable information computer crime
3. none of the above
4. The TRW Case is notable because:

a) The amount of dollars involved was so large

1. No one got caught
2. The real victims were TRW customers
3. A routine audit was responsible for detecting the fraud
4. Which of these is an acronym for computer crime legislation?

a) ACL

1. BART
2. CFAA
3. DDoS
4. Hacking involves:

a) Stealing carbons of credit cards

1. Destroying computer hardware
2. Gaining illegal entry to computer files from remote locations
3. Inserting a logic bomb in a computer program
4. A computer virus is:

a) A disease that computer programmers are very susceptible to

b) A small processing routine that the user accidentally introduces into the system

c) A misnomer, since unlike biological viruses, computer viruses cannot reproduce themselves

d) Harmless

1. Computer programs that can scan computer disks for virus-like coding are called:
	1. Antivirus software
	2. Virus software
	3. Detection software
	4. Friendly applets
2. All of the following are ways to thwart computer viruses *except*:

a) Acquire a vaccine or anti‑virus program

1. Do not download computer games from questionable sources
2. Maintain complete backup files
3. Buy shrink‑wrapped software from reputable sources
4. A small computer program that is stored on a web server and designed to run in conjunction with browser software is called a(n):

a) Applet

1. Logic bomb
2. Worm
3. Boot sector
4. Thwarting computer abuse can be enhanced by all of the following *except*:

a) Enlisting top-management support

1. Increasing employee awareness and education
2. Allowing only 10% of employees access to computers
3. Using strong passwords
4. In thwarting cybercrime, which of the following is true?
	* 1. It is not important to enlist the support of top management
		2. Many IT managers do not think cybercrime is very important
		3. Cybercrime mostly means controlling computer hardware
		4. Most cybercrime happens because of a failure of controls, not an absence of controls
5. Almost all computer criminals can be described as:
6. Professional criminals
7. Technical hackers possessing strong computer skills
8. White collar professional criminals
9. Amateurs who describe themselves as relatively honest
10. Most computer criminals who have been caught:
11. Have inferior educational backgrounds
12. Have superior educational backgrounds
13. Work for organized crime
14. Are ill suited to their jobs
15. A forensic accountant is an accountant who:
16. Performs autopsies on dead accountants
17. Tries to explain why some accounts become inactive
18. Investigates suspected fraud
19. Performs court-approved accounting tasks for bankrupt companies
20. Accounting “ethics” means:
21. Whatever the corporate manual says it means
22. Acting responsibly as long as no dollars are involved
23. Only being honest; everything else is up for grabs
24. Acting responsibly, no matter what
25. An example of a conflict-of-interest situation is:
26. Not working for a new company in a job similar to your last job
27. Not talking to outsiders about general business concerns
28. A decision where personal and corporate goals conflict
29. Refusing to use a new computer if your colleagues are not provided similar systems
30. Which of the following is *not* a common way to steal personal identity information?

a) Altering computer records

1. Using key logging software
2. Dumpster diving
3. Phishing
4. Which of the following is true?

a) Only the AICPA has drafted an ethical code of conduct

b) Computer crime only refers to manipulating a computer to dishonestly obtain money, property, or some other advantage of value

c) ACM society is an acronym meaning “association of corporate managers”

d) Ethical use of computers means realizing that the availability of a system does not convey its unrestricted use

1. Probably the most important federal legislation governing activities involving computers is:

a) CAN-SPAM Act of 2003

b) Federal Privacy Act of 1974

c) Computer Fraud and Abuse Act of 1986

d) Cyber Security Act of 1987

1. Which of the following is a primary reason why accountants should be concerned about cybercrime?

a) They might lose their job if they don’t detect cybercrime in their organization

b) They might lose their professional credibility and license if cybercrime continues for a long time in their organization and they do not detect it

c) They are responsible for designing, implementing, and monitoring the control procedures for AISs

d) all of the above are equally important

1. One of the most effective deterrents to prevent/discourage computer hacking is:

a) User education, that is, making potential hackers aware of the ethical issues involved in this sort of behavior

b) The USA Patriot Act of 2001

c) The Cyber Security Act of 1987

d) none of the above

1. Which of the following does *not* destroy data but merely replicates itself repeatedly until the user runs out of internal memory or disk space?

a) Computer virus

b) Worm program

c) Java applet

d) Salami technique

1. It is important to be able to recognize the symptoms of employee fraud. In practice, which of the following might be the best clue that fraud might be occurring?

a) Accounting irregularities

b) Internal control procedures that managers feel are inadequate

c) Anomalies that, together, seem unreasonable

d) Trial balances that almost always contain errors

1. One of the major crimes identified by the Computer Fraud and Abuse Act of 1986 is the intent to illegally obtain information or tangible property through the use of computers. Which of the following methods might accomplish this type of crime if the perpetrator can change data before, during, or after they are entered into a computer system?

a) Salami technique

b) Data diddling

c) Shoulder surfing

d) Trojan horse program

69. Acts such as dumpster diving, phishing, and smishing are all conducted to:

 a) Conduct a denial of service attack

 b) Disrupt computer services

 c) Get food

 d) Perform identify theft

70. The term “smishing” means:

 a) Conducting identify theft by using text messages on cell phones

 b) Attempting to appear unnoticeable for an illegal act

 c) Stealing small amounts of monies from several computer accounts

 d) Masquerading as a corporate manager in order to obtain useful information

71. A computer virus is different from a “Trojan Horse” because the virus can

a) Corrupt data

b) Alter programming instructions

c) Replicate itself

d) Erase executable files

72. Some firms and governmental organizations use *ethical hackers* to help find any vulnerabilities that could be exploited by a malicious hacker. Which of the following is also used to refer to ethical hacking?

a) Denial of service

b) Intrusion service

c) Penetration testing

d) Executable testing

73. Misappropriation of assets is:

a) A form of computer fraud involving the misapplication of account numbers.

b) The theft of assets, usually by employees

c) The proper recording of assets using debits

d) A form of computer abuse that is not a crime

74. The theft of millions of credit card numbers from customers of Target stores using malware is an example of:

a) Denial of service

b) Misappropriation of assets

c) Penetration testing

d) Hacking

75. Good computer security usually begins with:

a) Strong application controls

b) Enlisting the support of top management

c) Long jail sentences

d) Powerful microprocessors

**Matching Questions**

For the following terms find the correct definition below and place the letter of that response in the blank space next to the term. Each definition is used only once – there are three terms that are *not* used.

76. \_\_\_\_\_ shoulder surfing

77. \_\_\_\_\_ ACL

78. \_\_\_\_\_ CSI

79. \_\_\_\_\_ data diddling

80. \_\_\_\_\_ cookie

81. \_\_\_\_\_ dumpster diving

82. \_\_\_\_\_ EnCase

83. \_\_\_\_\_ CFAA

84. \_\_\_\_\_ salami technique

85. \_\_\_\_\_ Trojan horse

86. \_\_\_\_\_ firewall

87. \_\_\_\_\_ worm

**Definitions:**

1. Malicious software similar to a computer virus
2. An acronym for security institute that studies computer crime activities
3. The act of altering data that are entered into, or used by, a computer
4. A software program specifically designed for computer forensic investigations
5. Federal legislation aimed specifically at computer crime
6. A type of fraud in which the perpetrator steals small amounts from many different accounts
7. A technique for luring individuals to reveal their personal identification information
8. A software program or hardware device designed to prevent unauthorized data communications
9. A malicious software program embedded in another innocent-looking one
10. A type of bait used to lure computer users into sending money overseas
11. A small text file that stores information about your browsing habits and interests
12. Stealing personal information from trash cans
13. Auditing software often used to test computer data
14. Observing users as they enter passwords or other personal information to a computer
15. A strong computer password named after a Greek statue

**Short Answer Questions**

88. Define hacking.

89. Define computer virus.

90. Many say that cybercrime prevention begins with good policies and education of people. Discuss what it means to have good policies and good education.