

Test Bank for Corporate Cybersecurity 6th Boyle

TEST BANK SAMPLE PREVIEW

PUBLISHER

Pearson

COPYRIGHT

2025

RESOURCE TYPE

Test Bank

ISBN

9780135339268

Corporate Computer Security, 6e (Boyle/Panko)
Chapter 1 The Threat Environment

- 1) The process of protecting computer hardware, networks, data, and applications from attackers is called _____.
- A) cybersecurity
 - B) the threat environment
 - C) a data breach
 - D) a countermeasure

Answer: A

Page Ref: 16

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

- 2) If an attacker breaks into a corporate database and deletes critical files, this is an attack against the _____ security goal.
- A) confidentiality
 - B) integrity
 - C) availability
 - D) CIA

Answer: B

Page Ref: 20

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Moderate

- 3) Which of the following is a type of countermeasure?
- A) Ethical
 - B) Invisible
 - C) Detective
 - D) Sustainable

Answer: C

Page Ref: 21

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Moderate

- 4) The most common type of attack appears to be _____.
- A) phishing
 - B) compromised credentials

- C) cloud misconfiguration
- D) malicious insider

Answer: B

Page Ref: 17

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

5) When a threat succeeds in causing harm to a business it is called a _____.

- A) control
- B) countermeasure
- C) compromise
- D) corrective

Answer: C

Page Ref: 20

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Moderate

6) Three common core security goals are known collectively as FBI.

Answer: FALSE

Page Ref: 19

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

7) Costs for all threats are increasing annually.

Answer: FALSE

Page Ref: 19

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

8) Corrective countermeasures identify when a threat is attacking.

Answer: FALSE

Page Ref: 21

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

9) Most countermeasure controls are preventative controls.

Answer: TRUE

Page Ref: 21

Learning Objective: 1.1 Define the term *threat environment*

Difficulty: Easy

10) A _____ happens when an unauthorized person is able to view, alter, or steal secured data.

- A) countermeasure
- B) data breach
- C) safeguard
- D) compromise

Answer: B

Page Ref: 22

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

11) In 2022, _____ records were stolen.

- A) about 10 million
- B) nearly 5 billion
- C) more than 20 billion
- D) almost 50 billion

Answer: C

Page Ref: 22

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

12) IBM found that _____ percent of organizations have had more than one data breach.

- A) 17
- B) 25
- C) 61
- D) 83

Answer: D

Page Ref: 23

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

13) Which of the following is a direct cost of a data breach?

- A) Loss of reputation
- B) Abnormal customer turnover
- C) Legal fees
- D) Increased customer acquisition activities

Answer: C

Page Ref: 23

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

14) Which of the following is NOT a direct cost of a major data breach?

- A) Loss of reputation
- B) Notification costs
- C) Legal fees
- D) Detection

Answer: A

Page Ref: 23

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

Difficulty: Easy

15) More than 67 percent of data breaches come from hackers _____.

- A) trying to make money
- B) engaging in industrial espionage
- C) getting personal revenge
- D) making a social statement

Answer: A

Page Ref: 24

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

16) Stolen information is commonly used for _____.

- A) credit card fraud
- B) identity theft

- C) false claims
- D) data mismanagement

Answer: A

Page Ref: 24

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

- 17) Understanding how data breaches happen _____.
- A) is the first step in protecting yourself from data breaches
 - B) is impossible, since hackers are continually developing new tools
 - C) will make you more susceptible to future attacks
 - D) is a waste of time as attacks are inevitable these days

Answer: A

Page Ref: 25

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

- 18) A targeted phishing attack aimed at a single individual is called _____.
- A) spear phishing
 - B) a Trojan horse
 - C) a virus
 - D) spam

Answer: A

Page Ref: 26

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

- 19) The Target data breach helped impact a shift from swipe cards to _____.
- A) EMV-compliant smart cards
 - B) POS systems
 - C) keystroke logger
 - D) rootkits

Answer: A

Page Ref: 27

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

- 20) One of the long-lasting effects of the data breach to Target was _____.
A) loss of money
B) loss of customer confidence
C) loss of merchandise
D) employee dissatisfaction

Answer: B

Page Ref: 27

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

- 21) Data breaches are always the result of hackers in distant locations.

Answer: FALSE

Page Ref: 25

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

- 22) Paying for notification and detection are indirect costs associated with a data breach.

Answer: FALSE

Page Ref: 23

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Moderate

- 23) In 2022, the average global cost of a data breach was down 13 percent from 2020.

Answer: FALSE

Page Ref: 23

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

- 24) Rogue internal employees typically have a more difficult time stealing data than do external hackers.

Answer: FALSE

Page Ref: 25

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

25) The Target data breach affected 30 percent of the population of the U.S.

Answer: TRUE

Page Ref: 25

Learning Objective: 1.2 Describe the impact of *data breaches*

Difficulty: Easy

26) _____ are particularly dangerous because of their extraordinary knowledge and access.

- A) Financial professionals
- B) IT employees
- C) CEOs
- D) Data entry clerks

Answer: B

Page Ref: 29

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Moderate

27) Sabotage is defined as _____.

- A) the destruction of hardware, software, or data
- B) breaking into computers using stolen credentials or other fraudulent means
- C) the misappropriation of assets
- D) the theft of the company's intellectual property

Answer: A

Page Ref: 30

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Challenging

28) In _____, a perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest.

- A) fraud
- B) hacking
- C) abuse
- D) extortion

Answer: D

Page Ref: 31

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

29) _____ consists of activities that violate a company's IT use and/or ethics policies.

- A) Abuse
- B) Fraud
- C) Extortion
- D) Hacking

Answer: A

Page Ref: 31

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

30) Which of the following is considered a trade secret?

- A) Product formulations
- B) Patents
- C) Trade names
- D) Trademarks

Answer: A

Page Ref: 30

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

31) Penalties for hacking are significantly different if you are attempting to steal a million dollars or attempting to steal nothing of value.

Answer: FALSE

Page Ref: 30

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

32) Downloading pornography can invoke a sexual harassment lawsuit.

Answer: TRUE

Page Ref: 31

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

33) You have access to your home page on a server. By accident, you discover that if you hit a certain key, you can get into someone else's files. You spend just a few minutes looking around. This is hacking.

Answer: TRUE

Page Ref: 30

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Moderate

34) The motivation for hacking is irrelevant.

Answer: TRUE

Page Ref: 30

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

35) Unlike employees, contract workers do not constitute a threat to a business.

Answer: FALSE

Page Ref: 32

Learning Objective: 1.3 Describe threats from *employees* and *ex-employees*

Difficulty: Easy

36) Malware generically means _____.

- A) evil software
- B) unauthorized access
- C) abusive behavior
- D) misappropriated information

Answer: A

Page Ref: 32

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

37) _____ are programs that attach themselves to legitimate programs.

- A) Viruses
- B) Worms
- C) Payloads
- D) Direct-propagation worms

Answer: A

Page Ref: 32

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Easy

- 38) Direct propagation worms _____.
- A) take advantage of security weaknesses in software.
 - B) require action on the user's part to be spread
 - C) have a far less aggressive spreading mode than other malware
 - D) cannot use the infected computer as a base to jump to other computers

Answer: A

Page Ref: 34

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Difficult

- 39) What is a payload?
- A) Malicious software that blocks access to a system or data until money is paid to the attacker
 - B) A generic name for any "evil software"
 - C) A piece of code that does damage
 - D) A program that gives an attacker remote control of your computer

Answer: C

Page Ref: 35

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Difficult

- 40) What does RAT stand for?
- A) realistic artificial intelligence
 - B) remote access Trojan
 - C) ransomware after theft
 - D) rootkit appropriation threat

Answer: B

Page Ref: 36

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

- 41) A _____ is a small program that, after installed, downloads a larger attack

program.

- A) rootkit
- B) keystroke logger
- C) downloader
- D) Trojan horse

Answer: C

Page Ref: 36

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

42) Which of the following is FALSE about rootkits?

- A) Rootkits are seldom caught by ordinary antivirus programs.
- B) Rootkits take over the root account of a computer.
- C) Rootkits use a root account's privileges to hide themselves.
- D) Rootkits are typically less of a threat than Trojan horses.

Answer: D

Page Ref: 38

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Difficult

43) _____ take advantage of flawed human judgment by convincing a victim to take actions that are counter to security policies.

- A) Phishing attacks
- B) Hoaxes
- C) Social engineering attacks
- D) Spear phishing attacks

Answer: C

Page Ref: 39

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

44) You receive an e-mail that seems to come from your bank. Clicking on a link in the message takes you to a website that seems to be your bank's website. However, the website is fake. This is called _____.

- A) a hoax
- B) social engineering
- C) spear fishing
- D) phishing

Answer: D

Page Ref: 39

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

- 45) You receive an e-mail that appears to come from a frequent customer. It contains specific information about your relationship with the customer. Clicking on a link in the message takes you to a website that seems to be your customer's website. However, the website is fake. This is an example of _____.
- A) social engineering
 - B) spear fishing
 - C) phishing
 - D) a hoax

Answer: B

Page Ref: 39

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

- 46) BEC attacks account for about a quarter of social engineering breaches.

Answer: TRUE

Page Ref: 40

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Easy

- 47) Spear fishing attacks tend to appeal broadly to many people so they can dupe as many victims as possible.

Answer: FALSE

Page Ref: 40

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Moderate

- 48) Cookies are small text strings stored on your own personal computer.

Answer: TRUE

Page Ref: 38

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Easy

- 49) Data mining spyware searches through your disk drives for the same types of information sought by keystroke loggers, and sends this information to the adversary.

Answer: TRUE

Page Ref: 38

Learning Objective: 1.4 Describe threats from *malware* writers

Difficulty: Easy

- 50) Most traditional external attackers were primarily motivated by _____.
A) the thrill of breaking in
B) making money through crime
C) stealing personal identity data
D) capturing thousands and thousands of credit card numbers

Answer: A

Page Ref: 40

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

- 51) ICMP Echo messages are often used in _____.
A) port scanning
B) IP address scanning
C) spoofing
D) DDoS attacks

Answer: B

Page Ref: 42

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Moderate

- 52) When a hacker sends a first round of probe packets to find hosts that are active, the attacker is sending _____ probes.
A) IP address scanning
B) a chain of attack
C) piggybacking

D) IP address spoofing

Answer: A

Page Ref: 42

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Moderate

53) Watching someone type their password to learn the password is called _____.

- A) piggybacking
- B) a chain of attack
- C) social engineering
- D) shoulder surfing

Answer: D

Page Ref: 45

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

54) In a DoS attack, the botmaster is also known as a _____.

- A) handler
- B) hacker
- C) hoax
- D) rootkit

Answer: A

Page Ref: 46

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

55) The specific attack method an attacker uses to break into a computer is called the attacker's _____.

- A) spoof
- B) exploit
- C) piggyback
- D) chain of attack

Answer: B

Page Ref: 43

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Moderate

56) By demonstrating their ability to break into well-defended hosts, hackers could increase their reputation among their peers.

Answer: TRUE

Page Ref: 41

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

57) All packets can be spoofed.

Answer: FALSE

Page Ref: 44

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

58) In response to a chain of attack, victims can often trace the attack back to the final attack computer.

Answer: TRUE

Page Ref: 44

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

59) Following someone through a secure door without entering a pass code is called piggybacking.

Answer: TRUE

Page Ref: 45

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

60) Script kiddies are typically hacker experts.

Answer: FALSE

Page Ref: 47

Learning Objective: 1.5 Describe traditional external *hackers* and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks

Difficulty: Easy

61) _____ are the most common external attackers who attack to make money illegally.

- A) Hackers
- B) Career criminals
- C) Script kiddies
- D) IT or security employers

Answer: B

Page Ref: 48

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Easy

62) Many e-commerce companies will not ship to certain countries because of a high rate of consumer fraud. To get around this, criminal gangs engage _____ in the United States.

- A) transshippers
- B) APTs
- C) black-market websites
- D) IP address spoofing

Answer: A

Page Ref: 49

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Easy

63) _____ programs reward researchers for finding vulnerabilities.

- A) Transshipper
- B) APT
- C) Black-market website
- D) Bug bounty

Answer: D

Page Ref: 50

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Moderate

- 64) Criminals can use crime-as-a-service to _____ that cyber criminals must perform as part of their criminal operations.
- A) avoid detection of the hacking
 - B) hide the evidence
 - C) outsource some of the illegal activities
 - D) automate many of the labor-intensive functions

Answer: D

Page Ref: 51

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Moderate

- 65) Credit card theft is also known as _____.
- A) extortion
 - B) click fraud
 - C) bug bounty
 - D) carding

Answer: D

Page Ref: 53

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Moderate

- 66) What does APT stand for?
- A) advanced persistent threat
 - B) artificial phishing trap
 - C) adaptive property transshipper
 - D) attacks per text

Answer: A

Page Ref: 50

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Easy

67) Which of the following is likely the most common criminal attack on individuals?

- A) Bank account theft
- B) Credit card number theft
- C) Spoofing
- D) Spam

Answer: B

Page Ref: 53

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Moderate

68) Cybercrime proceedings surpassed those from illegal drug sales in 2005.

Answer: TRUE

Page Ref: 48

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Easy

69) Identify theft can (and does) happen to individuals, but it is not a worry or risk that corporations have.

Answer: FALSE

Page Ref: 54

Learning Objective: 1.6 Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation

Difficulty: Easy

70) A company's website and Facebook pages may divulge information that competitors may seek out. This is known as _____.

- A) public intelligence gathering
- B) spoofing
- C) bug bounty
- D) carding

Answer: A

Page Ref: 55

Learning Objective: 1.7 Describe the types of attacks that could come from corporate *competitors*

Difficulty: Easy

71) Russia is one of the countries cited as being the most capable cyber actors actively engaged in economic espionage.

Answer: TRUE

Page Ref: 55

Learning Objective: 1.7 Describe the types of attacks that could come from corporate *competitors*

Difficulty: Easy

72) Commercial espionage is limited to corporate competitors.

Answer: FALSE

Page Ref: 55

Learning Objective: 1.7 Describe the types of attacks that could come from corporate *competitors*

Difficulty: Easy

73) Cyberwar consists of computer-based attacks made by _____.

- A) multinational corporations
- B) state, regional, and local governments
- C) national governments
- D) private citizens

Answer: C

Page Ref: 56

Learning Objective: 1.8 Distinguish between *cyberwar* and *cyberterror*

Difficulty: Moderate

74) Cyberwar attacks can be launched without engaging in physical hostilities and still do significant damage.

Answer: TRUE

Page Ref: 57

Learning Objective: 1.8 Distinguish between *cyberwar* and *cyberterror*

Difficulty: Moderate

75) It is most common for cyberterrorists to recruit through face-to-face means.

Answer: FALSE

Page Ref: 57

Learning Objective: 1.8 Distinguish between *cyberwar* and *cyberterror*

Difficulty: Easy