Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

SKU: 9781506347257-TEST-BANK

Chapter 2: What Is Cybersecurity?

Test Bank

Multiple Choice

1. In 1988, the Defense Advances Research Projects Agency (DARPA) created the _____ with the goal of striving for a safer and stronger Internet for all Americans.
a. Computer Emergency Readiness Team
b. North American Aerospace Defense Command
c. National Security Agency
d. Advanced Research Projects Agency Network
Ans: A
Learning Objective: 2-2: Analyze the origin of cyberspace legislation and the direction it is headed in the future.
Cognitive Domain: Knowledge
Answer Location: Origins and Nature of Cybersecurity
Difficulty Level: Easy

2. In 1987, the _____ strengthened the security measures for online systems.
a. Federal Computer Systems Protection Act
b. Computer Security Act
c. Homeland Security Act
d. Cybersecurity Enhancement Act
Ans: B
Learning Objective: 2-2: Analyze the origin of cyberspace legislation and the direction it is headed in the future.
Cognitive Domain: Knowledge
Answer Location: Origins and Nature of Cybersecurity
Difficulty Level: Medium

3. Submarine Network Policy is used to secure devices at the _____ level.
a. local
b. state
c. federal
d. corporate
Ans: D
Learning Objective: 2-4: Discuss the role that wireless networks have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Securing Your Wi-Fi in a Wireless World
Difficulty Level: Medium

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

4. _____ is a bacterial disease, weaponized in powder form, which was sent to various television studios and congressional offices via mail in the early 2000s.
a. Botulism
b. Anthrax
c. Cholera
d. Ebola
Ans: B
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Knowledge
Answer Location: Definition of Cybersecurity
Difficulty Level: Easy

5. The _____ is responsible for collecting and decrypting threats both physical and cyber via the use of Signal Intelligence.
a. Central Intelligence Agency
b. Federal Bureau of Investigation
c. National Security Agency
d. Department of Homeland Security
Ans: C
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Knowledge
Answer Location: Definition of Cybersecurity
Difficulty Level: Easy

6. The role of the _____ was extended in the Cybersecurity Enhancement Act of 2014.
a. Secretary of Labor
b. Secretary of Treasury
c. Secretary of State
d. Secretary of Commerce
Ans: D
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Knowledge
Answer Location: Definition of Cybersecurity
Difficulty Level: Easy

7. Hacking cars or other means of transportation, such as airplanes, is an example of a security issue seen in which of the following techniques?
a. Man in the Cloud
b. Man in the Internet of Things
c. Man in the App
d. Man in the Browser
Ans: B

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Easy

8. Which of the following themes within the cybersecurity conceptualization literature was NOT identified by Craigen and his team?
a. events
b. human engagement
c. funding
d. technological solutions
Ans: C
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Application
Answer Location: Definition of Cybersecurity
Difficulty Level: Medium

9. Which of the following was NOT identified as a recommendation for increasing automotive cybersecurity?
a. third-party testing
b. aesthetic design
c. internal monitoring systems
d. segmented architecture
Ans: B
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Application
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Medium

10. According to General Michael Hayden, a cybersecurity knowledge gap exists between _____.
a. youthful generation and older generation
b. men and women
c. individuals of different ethnicities
d. private- and public-sector employees
Ans: A
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Application
Answer Location: Definition of Cybersecurity
Difficulty Level: Medium

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

11. The _____ Computer Emergency Response Team (CERT) investigated the cyber intrusion that became known as Moonlight Maze.
a. Navy's
b. Marines'
c. Army's
d. Air Force's
Ans: D
Learning Objective: 2-4: Discuss the role that wireless networks have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Knowledge
Answer Location: Overview of Cyberspace Intrusions
Difficulty Level: Easy

12. According to the text, dams, railways, and power plants are considered _____.
a. businesses
b. infrastructures
c. governments
d. organizations
Ans: B
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.
Cognitive Domain: Knowledge
Answer Location: Cybersecurity Policies
Difficulty Level: Easy

13. Work-for-hire hackers who work for private security corporations are also referred to as _____.
a. blue teams
b. black teams
c. red teams
d. green teams
Ans: C
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.
Cognitive Domain: Comprehension
Answer Location: Cybersecurity Policies
Difficulty Level: Easy

14. All of the following are considered public sector entities EXCEPT _____.
a. NSA
b. CIA
c. FusionX
d. DHS
Ans: C
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Cognitive Domain: Knowledge
Answer Location: Cybersecurity Policies
Difficulty Level: Easy

15. _____ became notorious for being the one of the first cybersecurity intrusions to illustrate how vulnerable our technology is to malicious infiltration.
a. Titan Rain
b. Moonlight Maze
c. Solar Sunrise
d. GhostNet
Ans: B
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Knowledge
Answer Location: Overview of Cyberspace Intrusions
Difficulty Level: Easy

16. _____ occur when a computer system is accessed without permission.
a. Distributed denial of services
b. Rogue access points
c. Micro-segments
d. Network intrusions
Ans: D
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Network-Based Attacks
Difficulty Level: Easy

17. _____ refers to attacks where a mass email is sent to multiple computers, requesting personal information be sent to a specific location.
a. Phishing
b. Distributed denial of service
c. Malware
d. Keylogging
Ans: A
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Network-Based Attacks
Difficulty Level: Easy

18. _____ allowing individuals to access secured networks without the owners' knowledge is also known as a backdoor.
a. Noisy neighbors
b. Phishing attacks

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

c. Rogue access points
d. Man-in-the-middle attacks
Ans: C
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Wireless Attacks
Difficulty Level: Easy

19. Which of the following types of attacks can also happen accidentally?
a. phishing
b. man-in-the-middle
c. malware
d. noisy neighbors
Ans: D
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Application
Answer Location: Wireless Attacks
Difficulty Level: Easy

20. The interception of a message by a third party is also referred to as a _____ attack.
a. phishing
b. human error
c. noisy neighbor
d. man-in-the-middle
Ans: D
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Wireless Attacks
Difficulty Level: Easy

21. The _____ technique, also referred to as a banking Trojan, operates in the background of the computer by modifying banking transactions.
a. man-in-the-middle
b. WiFi eavesdropping
c. man-in-the-browser
d. man-in-the-cloud
Ans: C
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Easy

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

22. The _____ technique targets file-sharing tools, such as Google Drive.
a. man-in-the-middle
b. man-in-the-cloud
c. man-in-the-browser
d. WiFi eavesdropping
Ans: B
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Easy

23. The _____ technique targets devices that can be connected, such as car alarms, thermostats, etc.
a. man-in-the-IoT
b. man-in-the-cloud
c. man-in-the-browser
d. WiFi eavesdropping
Ans: A
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Easy

24. Making mistakes that can lead to security vulnerabilities is also referred to as _____.
a. malicious intent
b. human error
c. interference
d. espionage
Ans: B
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Wireless Attacks
Difficulty Level: Medium

25. The creation of _____ has led to the creation of new hacking/fraudster built-in malware techniques that can target users via smartphones and tablets.
a. file sharing tools
b. messaging tools
c. apps
d. social media
Ans: C

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Man-in-the-Middle Attacks
Difficulty Level: Medium

True/False

1. The Computer Security Act was one of the first legislations to advance the protection of federal computers.
Ans: T
Learning Objective: 2-2: Analyze the origin of cyberspace legislation and the direction it is headed in the future.
Cognitive Domain: Knowledge
Answer Location: Origins and Nature of Cybersecurity
Difficulty Level: Easy

2. According to the text, preparing for a cyberattack was a top priority for national security in the late 1980s.
Ans: F
Learning Objective: 2-2: Analyze the origin of cyberspace legislation and the direction it is headed in the future.
Cognitive Domain: Knowledge
Answer Location: Origins and Nature of Cybersecurity
Difficulty Level: Easy

3. The aftermath of 9/11 led to an increase in cybersecurity strategies.
Ans: T
Learning Objective: 2-2: Analyze the origin of cyberspace legislation and the direction it is headed in the future.
Cognitive Domain: Knowledge
Answer Location: Origins and Nature of Cybersecurity
Difficulty Level: Easy

4. Critical infrastructures include transportation, electrical grid system, and banking systems.
Ans: T
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Comprehension
Answer Location: Definition of Cybersecurity
Difficulty Level: Easy

5. Defining cybersecurity is not an issue in the academe.
Ans: F

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Comprehension
Answer Location: Definition of Cybersecurity
Difficulty Level: Easy

6. The National Cybersecurity and Communications Integration Center works alone in reducing the probability and the damage caused by cyberattacks.
Ans: F
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.
Cognitive Domain: Comprehension
Answer Location: Cybersecurity Policies
Difficulty Level: Medium

7. Malware is readily available for purchase and/or download.
Ans: T
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Knowledge
Answer Location: Overview of Cyberspace Intrusions
Difficulty Level: Easy

8. The majority of critical infrastructure in the United States is owned by the public sector.
Ans: F
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.
Cognitive Domain: Knowledge
Answer Location: Cybersecurity Policies
Difficulty Level: Medium

9. White hat hackers work for private corporations to expose vulnerabilities in their security systems.
Ans: T
Learning Objective: 2-3: Differentiate between private and public-sector cybersecurity and the pros and cons of each.
Cognitive Domain: Comprehension
Answer Location: Cybersecurity Policies
Difficulty Level: Easy

10. According to the text, network attacks are attractive because they can go undetected and the perpetrators are difficult to trace.
Ans: T
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Cognitive Domain: Comprehension
Answer Location: Network-Based Attacks
Difficulty Level: Medium

Essay

1. Explain the difficulties in defining cybersecurity.
Ans: A strong answer will contain the issues of conceptualization and should provide an example of how conceptualization can differ depending on the context, such as the one identified in the text (criminal justice standpoint).
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Analysis
Answer Location: Definition of Cybersecurity
Difficulty Level: Hard

2. Describe the cybersecurity gap. Do you agree with the assertion of former Central Intelligence Agency director General Michael Hayden that there is a cybersecurity knowledge gap? Why or why not?
Ans: Answers will vary. However, a strong answer will include the differentiation between technological use among youthful and older generations.
Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Analysis
Answer Location: Definition of Cybersecurity
Difficulty Level: Medium

3. Identify the five dominant themes within the cybersecurity conceptualization literature. Which of these do you think is predominant in the conceptualization literature? Why?
Ans: Answers will vary. A good answer will identify each of the following.

1. Technological solutions
2. Events
3. Strategies, procedures, and methods
4. Human engagement
5. Referent objects (of security)

Learning Objective: 2-1: Understand the evolving nature of the term *cybersecurity* and the challenges presented with it.
Cognitive Domain: Comprehension
Answer Location: Definition of Cybersecurity
Difficulty Level: Medium

4. Identify and describe the two main forms of network-based attacks. How are they different? Use examples to differentiate the two.
Ans: A strong answer will include the definition of both untargeted and targeted attacks, in addition to their differences (victims, random versus chosen, etc.).

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank

Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Network-Based Attacks
Difficulty Level: Medium

5. Identify the benefits of wireless technology and the associated risks/vulnerabilities.
Ans: A strong answer will include benefits such as convenience, ease of access, productivity, flexibility, etc. Associated risks can include less security, human error, rogue access points, noisy neighbors, and man-in-the-middle attacks.
Learning Objective: 2-4: Discuss the role that wireless networks (Wi-Fi) have played in making the issue of cybersecurity even more complex.
Cognitive Domain: Comprehension
Answer Location: Wireless Attacks
Difficulty Level: Medium

Cyberspace Cybersecurity and Cybercrime 1st edition Kremling Test Bank