Test Bank for Developing Cybersecurity Programs and Policies in an AI-Driven World 4th Santos

Developing Cybersecurity Programs and Policies in an AI-Driven World **(Santos)**
Chapter 1 Understanding Cybersecurity Policy and Governance

1) Which of the following elements ensures a policy is enforceable?
A) Compliance can be measured.
B) Appropriate sanctions are applied when the policy is violated.
C) Appropriate administrative, technical, and physical controls are put in place to support the policy.
D) All of the above
Answer: D

2) Which of the following is typically not a component of cybersecurity programs and policies?
A) Oversight of cyber risk management
B) Sharing of threat intelligence
C) Implementation of traditional information security measures
D) Conducting incident response and digital forensics
Answer: C

3) Which of the following is an example of an information asset?
A) Business plans
B) Employee records
C) Company reputation
D) All of the above
Answer: D

4) Policy implementation and enforcement are part of which of the following phases of the cybersecurity policy life cycle?
A) Develop
B) Review
C) Adopt
D) Publish
Answer: C

5) Which of the following is the correct order of the cybersecurity policy life cycle?
A) Review, develop, adopt, publish
B) Develop, publish, adopt, review
C) Publish, develop, review, adopt
D) Review, adopt, develop, publish
Answer: B

6) Endorsed is one of the seven policy characteristics. Which of the following statements best describes endorsed?
A) The policy is supported and followed by management.
B) The policy is accepted by the organization's employees.
C) The policy is mandatory; compliance is measured; and appropriate sanctions are applied.
D) The policy is regulated by the government.

Answer: A

7) Which of the following is the outcome of policy review?
A) Retirement or renewal
B) Retirement or reauthorization
C) Renewal or reauthorization
D) None of the above
Answer: B

8) Which strategy is commonly used to protect network and corporate assets in cybersecurity?
A) Single-layered security approach
B) Cross-boundary defense-in-depth strategy
C) Random implementation of security controls
D) Reliance solely on firewalls and IPS
Answer: B

9) Which of the following statements is *not* true?
A) Policies should require only what is possible.
B) Policies that are no longer applicable should be retired.
C) All guiding principles and corporate cultures are good.
D) Guiding principles set the tone for a corporate culture.
Answer: C

10) Which of the following is *not* one of the six key tasks of the policy development phase?
A) Approve
B) Write
C) Communicate
D) Authorize
Answer: C

11) The United States Department of Homeland Security defines how many critical infrastructure sectors?
A) 16
B) 14
C) 20
D) 17
Answer: A

12) Which of the following is the seminal tool used to protect both our critical infrastructure and our individual liberties?
A) Information security
B) Society
C) Physical security
D) Policy
Answer: D

13) Which of the following can be defined as the shared attitudes, goals, and practices that characterize a company, corporation, or institution?
A) Regulations
B) Corporate culture
C) Cybersecurity policy
D) Guiding principles
Answer: B

14) Which of the following is a collection of articles and amendments that provide a framework for the American government and define citizens' rights?
A) The Constitution
B) The Torah
C) Data Protection Act
D) Consumer Credit Act
Answer: A

15) Which layer in the defense-in-depth strategy includes firewalls, IDS/IPS devices, segmentation, and VLANs?
A) Physical security
B) Network security
C) Perimeter security
D) Application security
Answer: C

16) Which of the following is another term for statutory law?
A) Legislation
B) Regulation
C) Policy
D) Governance
Answer: A

17) Which of the following federal legislations, also known as the Financial Modernization Act of 1999, was created to reform and modernize the banking industry by eliminating existing barriers between banking and commerce?
A) HITECH
B) HIPAA
C) FERPA
D) GLBA
Answer: D

18) Which major regulation entity within the European Union (EU) was created to maintain a single standard for data protection among all member states in the EU?
A) Directive on Security of Network and Information Systems (the NIS Directive)
B) EU General Data Protection Regulation (GDPR)
C) European Union Agency for Network and Information Security (ENISA)
D) The Consumer Credit Regulations 2010

Answer: B

19) Which key task in the policy development phase requires the authors to consult with internal and external experts, including legal counsel, human resources, compliance, cybersecurity and technology professionals, auditors, and regulators?
A) Writing
B) Authorizing
C) Vetting
D) Planning
Answer: C

20) Which key task in the policy adoption phase is the busiest and most challenging task of all?
A) Implementation
B) Enforcement
C) Monitoring
D) Education
Answer: A