CyberRookie CSX Fundamentals - Mock Exam 1

Friday, September 13, 2019   2:32 PM

Section 1- INTRODUCTION TO CYBERSECURITY

1. The objective of information security is threefold, it involves:

a) Availability, security, assurance

b) Confidentiality, integrity, availability

c) Cyber assurance, integrity, hacking

d) None of the above

2. The terms "cybersecurity" and "information security" are often used interchangeably, but in reality, cybersecurity is part of _____.:

a) Network security

b) Data security

c) Information security

d) Enterprise security

3. Controls used to protect assets, reduce _____ and _____ and/or reduce risk to an acceptable level.

a) Security, protection

b) Threats, weaknesses

c) Cost, security

d) Vulnerabilities, impacts

4. The National Institute of Standards and Technology (NIST) identifies five keys functions necessary for protection of digital assets, they are:

a) Identify, security, protect, detect, standards

b) Respond, identify protect, detect, recover

c) Password, policies, standards, identity, culture

d) None of the above

5. Nonrepudiation refers to the concept of:

a) Delegating security

b) Removing all responsibility from cyber professionals

c) Refusing evidence

d) Ensuring that a message or other piece of information is genuine

6. Governance is the responsibility of _____ and _____

a) Cyber practitioners, network administrators

b) Government, lawyers

c) Data owners, system architects

d) Board of directors, senior management

7. An organization's executive management team is responsible for:

a) Ensuring that needed organizational functions, resources and supporting infrastructures are available and properly utilized to fulfill the directives of the board

b) Ensuring the IT operations is working in accordance to system specifications

c) Ensuring the IT departments is well organized and follows a cyber security framework in accordance to the executives and operational standards

d) None of the above

8. Some of the responsibilities of a CISO or CSO include:

a) Developing the security strategy

b) Ensuring that risk and business impact assessments are conducted

c) Directing and monitoring security activities

d) (a),(b),(c)

e) (a), (b)

f) None of the above

9. In most organizations cyber security is managed by a team, which may include – select the MOST accurate statement:

a) Subject matter experts, cybersecurity practitioners, security architects, administrators, digit forensics, vulnerability researchers and network specialist

b) Human resource, compliancy consultants, board of directors, CEO

c) External consultants

d) Network administrators and risk authority

10. Read the description and match column with correct word: (3 marks max)

Compliance

Risk Management

Governance

The responsibility of the board of directors and senior management of the organization

The coordination of activities that direct and control

The act of adhering to, and the ability to demonstrate adherence to,

Compliance

Risk Management

Governance

The responsibility of the board of directors and senior management of the organization

The coordination of activities that direct and control

The act of adhering to, and the ability to demonstrate adherence to,

11. Three common controls used to protect the availability of information are:

a) Redundancy, backups and access controls.

b) Encryption, file permissions and access controls.

c) Access controls, logging and digital signatures.

d) Hashes, logging and backups.

12. Select all that apply. Governance has several goals, including:

a) Providing strategic direction.

b) Ensuring that objectives are achieved.

c) Verifying that organizational resources are being used appropriately.

d) Directing and monitoring security activities.

e) Ascertaining whether risk is being managed properly

13. Choose three. According to the NIST cybersecurity framework, which of the following are considered keyfunctions necessary for the protection of digital assets?

a) Encrypt

b) Protect

c) Investigate

d) Recover

e) Identify

14. Which of the following is the best definition for cybersecurity?

A. The process by which an organization manages cybersecurity risk to an acceptable level

B. The protection of information from unauthorized access or disclosure

C. The protection of paper documents, digital and intellectual property, and verbal or visual communications

D. Protecting information assets by addressing threats to information that is processed, stored or transported by

internetworked information systems

15. Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation?

A. Board of directors

B. Executive committee

C. Cybersecurity management

D. Cybersecurity practitioners

16. Which of the following describes the activities required to identify the occurrence of a cybersecurity incident?

Data security, awareness/training, access control and processes/procedures

Communications, analysis and mitigation

Security continuous monitoring, detection and evaluating anomalies/incidents

Asset management, risk management and risk assessment

17. This key function ensures that organizational objectives and stakeholder needs are aligned with desired outcomes through effective decision making and prioritization.

Governance

Risk management

Risk mitigation

Risk assessment

18. The primary objective of cybersecurity is:

Protection of all company assets

Responding to security incidents

Protecting a company's digital assets

Managing risk through countermeasures and controls

19. Which activity ensures that business processes continue after a security incident?

Recovery

Detection

Response

Protection

20. Which of the following activities is associated with identifying digital assets?

Asset management

Awareness and training

Recovery management

Security continuous monitoring

21. Which of the following are responsibilities and/or duties of Governance, Risk Management and Compliance (GRC)? Select all that apply.

Adherence to required laws and regulations

Implementation of required procedures

Development of internal controls to mitigate risk

Adherence to voluntary contractual requirements.

22. In most information security organizations, which role sets the overall strategic direction?

Chief Security Officer (CSO) or Chief Information Security Officer (CISO)

Board of Directors

Individual contributors

Chief Information Security Officer (CISO)

23. Governance involves all of the following except:

Provide strategic direction

Ensure responsible use of company resources

Evaluate whether risk is managed appropriately

Implement contractual obligations

24. Which role is generally responsible for the design, implementation, management processes and technical controls within a security organization?

Cybersecurity practitioners

Board of Directors

Executive management

Senior information security management

25. Which of the following falls within the scope of risk management? Investment risk and cyber risk

Cyber risk, investment risk and financial risk

Cyber risk and financial risk

Only cyber risk

26. Which term describes the overall structure designed to protect an organization from disclosure of information to unauthorized users, improper modification of data, and non-access to systems?

Cybersecurity

Information security

Information risk management

27. All of the following statements are true except:

Cybersecurity is a component of information security

Cybersecurity deals with the protection of digital assets

Cybersecurity includes protection of paper documents

Cybersecurity should align with enterprise information security objectives

28. Risk management involves which of the following activities? Select all that apply.

Recognizing risk

Assessing impact and likelihood of risk

Ensuring information security objectives are achieved

Developing strategies to mitigate risk

29. Cybersecurity involves the protection of the following digital assets:

Networks, hardware and paper documents

Digital or intellectual property stored in someone's mind, verbal and visual communications

Information that is processed, stored or transported within internetworked information systems

Only digital intellectual property, verbal or visual communications

30. Which terms describe the overall concept of information security? Select all that apply.

Linear

Ongoing

Evolving

Systemic

Back

Next

Never submit passwords through Google Forms.