Cyber Security and Privacy, IIT Madras
Prof. Saji K Mathew

Week 5 Quiz
(All questions carry 1 point each)

1 . The primary function of a cybersecurity policy within an organization is to:

a. Define a rigid set of penalties for security violations.
b. Eliminate the need for ongoing security awareness training programs.
c. Dictate specific technical security controls for implementation.
d. Establish a comprehensive reference point for organizational cybersecurity practices.

Ans: d. Establish a comprehensive reference point for organizational cybersecurity practices.
Explanation: A well-crafted cybersecurity policy serves as a foundational document, outlining desired employee behaviors and security best practices. It's not focused solely on punishments, doesn't replace training, and allows flexibility in choosing specific controls.

2 . Which type of policy is related to an organization's strategic purpose, mission, and vision?

a. Issue-specific information security policies (ISSP)
b. Systems-specific information security policies (SysSP)
c. Enterprise information security policy (EISP)
d. Technical implementation policy

Ans: c.Enterprise information security policy (EISP)
Explanation: EISP policies are related to an organization's strategic purpose, mission, and vision, providing the overarching framework for its information security program.

3 . True or False: Standards are broad, abstract documents that provide detailed procedures for employees to comply with policies.

a.True
b.False

Ans: b.False
Explanation: Standards are more detailed statements of what must be done to comply with policy practices, while procedures and guidelines explain how employees will comply with policy.

4. Which of the following reflects the hierarchical top-down order of information security policies?

a.Enterprise > Issue-Specific > Systems-Specific
b.Systems-Specific > Issue-Specific > Enterprise
c.Issue-Specific > Enterprise > Systems-Specific
d.All three policy types are independent and unconnected.

Ans: a.Enterprise > Issue-Specific > Systems-Specific
Explanation: The hierarchy goes from broad organizational strategy (Enterprise) to specific technologies (Systems-Specific). Option (a) reflects this top-down order.

5. Which of the following components is typically included in the Enterprise Information Security Policy (EISP)?

a. Incident response procedures
b. Statement of purpose
c. Software development guidelines
d. Employee performance evaluations

Ans: b.Statement of purpose
Explanation: The Statement of Purpose is one of the key components of the EISP, providing clarity on the purpose and objectives of the policy.

6. True or False: Systems-specific security policies (SysSPs) can be separated into two general groups, managerial guidance SysSPs and technical specifications SysSPs.

a. True
b. False

Ans: a. True
Explanation: SysSPs can be separated into managerial guidance SysSPs and technical specifications SysSPs, or they can be combined into a single policy document that contains elements of both.

7. ___________ consists of details about user access and use permissions and privileges for an organizational asset or resource.
a. Access Control Lists
b. Configuration rules
c. Authorized access and usage of equipment
d. Authorization rules

Ans: a. Access Control Lists
Explanation: ACL include the specifications of authorization that govern the rights and privileges of users to a particular information asset.

8. True or False: Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the lowest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments.

a. True
b. False

Ans: b. False

Explanation: CCE focuses on the highest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments.

9. _________ are nonmandatory recommendations the employee may use as a reference in complying with a policy.

a. Practices
b. Procedures
c. Standards
d. Guidelines

Ans: d. Guidelines
Explanation: Guidelines are recommendations for compliance.

10. Creating "air gaps" to isolate critical systems is a cyber hygiene practice that focuses on:
    a. Installing the latest security patches.
    b. Strengthening user authentication.
    c. Segmenting networks for improved security
    d. Keeping complex passwords up-to-date.

Ans: c. Segmenting networks for improved security
Explanation : An air gap is a security measure that isolates a critical system from other networks and even the internet. This physical or logical separation makes it much harder for attackers to reach the isolated system, even if they breach the main network.