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

Week 6 Quiz
(All questions carry 1 point each)

1. A determination of the extent to which an organization's information assets are exposed to risk is known as:

a. Risk identification
b. Risk control
c. Risk assessment
d. Risk Management

Ans: c. Risk assessment
Explanation: Risk assessment enables organizations to identify and address potential threats and vulnerabilities proactively.

2. _____is the risk to information assets that remains even after current controls have been applied.

a. Risk appetite
b. Residual risk
c. Inherent risk
d. Contingency risk

Ans: b. Residual risk
Explanation: Residual risk is the risk that is left over after the risk management process has concluded.

3. Which of these is not a component of risk identification?

a. Plan & organize the process
b. Classify, value, & prioritize assets
c. Specify asset vulnerabilities
d. Determine loss frequency

Ans: d. Determine loss frequency
Explanation: Determine loss frequency (Likelihood) is a component of risk assessment.

4. The likelihood of an attack together with the attack frequency to determine the expected number of losses within a specified time range is known as:

a. Loss frequency
b. Attack success probability
c. Loss magnitude
d. Risk

Ans: a. Loss frequency
Explanation: Loss frequency is the probability that an organization will be the target of an attack, multiplied by the probability that the organization's information assets will be successfully compromised if attacked.

5. _____is an information attack that involves searching through a target organization's trash for sensitive information.

a. Shoulder surfing
b. Network sniffing
c. Dumpster diving
d. Watering hole attacks

Ans: c. Dumpster diving
Explanation: Dumpster diving is a cyberattack where the attacker obtains sensitive information or documents that you've negligently discarded in the trash.

6 . Risk management in cyber security involves three key steps. These steps are:

a. Monitoring, auditing, and reporting.
b. Identifying risks, assessing risk, and controlling risks.
c. Training employees, patching vulnerabilities, and using firewalls.
d. Investigating incidents, recovering data, and learning lessons.

Ans: b. Identifying risks, assessing risk, and controlling risks
Explanation: The core process of risk management involves identifying the organization's assets, & threats, assessing risks, and then taking steps to reduce the risks associated with those threats.

7 . The "attack surface" in cyber security is a visualization tool that helps to understand:

a. The effectiveness of different security tools.
b. The relationship between various types of threats and the organization's assets.
c. The complexity of the organization's network infrastructure.
d. The cost of implementing different security controls.

Ans: b. The relationship between various types of threats and the organization's assets.
Explanation: The attack surface visualizes the potential threats on the Y-axis and the organization's assets on the X-axis. This helps identify points of vulnerability and prioritize risk reduction efforts.

8. During the Risk Identification phase, assets are classified into which of the following categories?

a. Financial assets, Intellectual property, and Human resources
b. Assets, Liabilities, and Equity
c. Tangible assets, Intangible assets, and Fixed assets
d. People, Procedures, Data and information, Software, Hardware, and Networking elements

Ans: d. People, Procedures, Data and information, Software, Hardware, and Networking elements

Explanation: Risk Identification begins with self-examination and Identification of info assets (6 categories) including people, procedures, data and information, software, hardware and networking elements.

9. Which formula accurately represents the calculation of risk in cyber security risk assessment?

a. Risk = Loss frequency + Loss magnitude
b. Risk = Loss frequency x Loss magnitude + Measurement Uncertainty
c Risk = (% Risk Mitigated by Controls) / (Loss Frequency x Loss Magnitude)
d. Risk = Loss frequency - Loss magnitude + Measurement Uncertainty

Ans: b.Risk = Loss frequency x Loss magnitude + Measurement Uncertainty
Explanation: RISK is the Probability of a Successful Attack on the Organization (Loss Frequency = Likelihood ∗ Attack Success Probability) Multiplied by the Expected Loss from a Successful Attack (Loss Magnitude = Asset Value ∗ Probable Loss) Plus The Uncertainty of estimates of all stated values

10. You are a security analyst for a company that manages an online store with a customer database. Industry reports indicate a 10 percent chance of an attack this year, based on an estimate of one attack every 10 years. A successful attack could result in the theft of customer data. There is a 20% chance of the threat being able to materialize and achieve its objectives even in place of robust secure protection mechanisms. The customer database is most valued being an e-commerce company at 90 in a 1-100 scale. The IT department informed that 60% of the assets will be exposed after a successful attack. The estimation of measurements is 80% accurate. Calculate the risk associated to the asset with a potential SQL injection attack.

a. 3.756
b. 4.196
c. 3.276
d. 1.296

Ans: d. 1.296

Explanation:
RISK is the Probability of a Successful Attack on the Organization (Loss Frequency = Likelihood ∗ Attack Success Probability) Multiplied by the Expected Loss from a Successful Attack (Loss Magnitude = Asset Value ∗ Probable Loss) Plus The Uncertainty of estimates of all stated values

Likelihood :0.1, Attack Success Probability: 0.2
Loss Frequency: 0.1 * 0.2 = 0.02
Loss Magnitude: 0.6 * 90 = 54
Risk = 0.02 * 54 + 20% = 1.296

(0.1*0.2) * (90*0.6) + 20% => 0.02*54 +20% => 1.08 +0.216=1.296