Ruth Abeselom

IT Security Management

1.2 What is the difference between passive and active security threats?

An active attack is a type of security breach where the attacker initiates direct communication with the system or network they are targeting. In this attack, a hacker uses unauthorized commands or malicious traffic injection to try and alter or interfere with the operation of the system or network. It can cause serious harm and financial loss for the targeted organization by undermining data integrity and decreasing system resource availability. On the other hand, a passive attack occurs when an attacker monitors the communication between the target system and the network while maintaining indirect contact with the target system. This attack involves an attacker monitoring, intercepting, or eavesdropping on data communications without altering or impacting them. A passive attack's primary goal is to obtain unauthorized access to private or sensitive data without being discovered. Since they don't alter data or interfere with system functions, they can be hard to detect.

14.1 Define IT security management.

The practice of safeguarding an organization's assets and data against potential dangers is known as information security management. The protection of data availability, integrity, and confidentiality is one of the main objectives. Information security management is determining the possible risks to an organization, evaluating the likelihood and potential consequences of those risks, and creating and putting into operation mitigation strategies that minimize risks and threats. This necessitates effective asset identification and valuation stages, such as determining the value of confidentiality, integrity, availability, and asset replacement.

14.13 Define consequence and likelihood.

The likelihood is just how likely the risk is to occur, whereas the consequence is the impact on the organization. In terms of IT security management, likelihood refers to the possibility that an attack will occur. Since the risk of any threat is dependent on the chance of it occurring (likelihood), and the impact of an occurrence (consequence). Consequence discusses the effects on the organization that might arise if the given threat emerges. Organizations can use the risk likelihood versus consequence indication to evaluate how well they are handling their risk agenda.

Risk = (Probability that threat occurs) x (Cost to organization)

15.1 Define security control or safeguard.

Security controls, often known as safeguards, are policies, processes, or other mechanisms that can lessen vulnerability, prevent unwanted incidents from happening, identify undesired incidents, and make recovery easier. The application of a thorough set of security measures that address personnel, physical, and cyber security is necessary for the protection of information. Security controls encompass operational, technical, and management policies and procedures that aim to reduce an organization's exposure to certain risks by preventing a threat source's ability to take advantage of certain vulnerabilities.

15.4 List the steps we discuss for selecting and implementing controls

- Prioritize Actions
- Evaluate Recommended Control Options
- Conduct Cost-Benefit Analysis
- Select Controls
- Assign Responsibility
- Develop Safeguard Implementation Plan
- Implement Selected Controls