DAY 7 {2}

Phishing attacks:

Risk Level: High

Description: Employees may be tricked into revealing sensitive information or clicking on malicious links.

Recommendation: Implement phishing simulation training for employees, and conduct regular security awareness campaigns.

Pretexting:

Risk Level: Medium

Description: Attackers may pose as IT staff or vendors to gain access to sensitive information or systems.

Recommendation: Implement a verification process for vendors and IT staff, and conduct regular security awareness campaigns.

Baiting:

Risk Level: Low

Description: Employees may be tempted to insert infected USB drives or other devices into company computers.

Recommendation: Implement a policy prohibiting the use of unauthorized USB drives, and conduct regular security awareness campaigns.

Quid pro quo:

Risk Level: Medium

Description: Attackers may offer a service or benefit in exchange for sensitive information.

Recommendation: Implement a policy prohibiting the exchange of sensitive information for services or benefits, and conduct regular security awareness campaigns.

Whaling:

Risk Level: High

Description: Targeted attacks on high-level executives or officials to gain access to sensitive information.

Recommendation: Implement targeted security awareness campaigns for high-level executives and officials, and provide additional security measures for their accounts and devices.

Insufficient training:

Risk Level: High

Description: Employees may not be adequately trained to recognize and respond to social engineering attacks.

Recommendation: Provide regular security awareness training for all employees, and conduct phishing simulation exercises to test their knowledge.

DAY 7 {2}

Lack of incident response plan:

Risk Level: High

Description: The organization may not have a plan in place to respond to social engineering attacks.

Recommendation: Develop and implement an incident response plan that includes procedures for responding to social engineering attacks.

Physical Threats Vulnerabilities:

Unsecured physical access:

Risk Level: High

Description: Unauthorized individuals may gain access to sensitive areas or devices.

Recommendation: Implement access controls, such as biometric authentication or smart cards, and conduct regular security audits.

Tailgating:

Risk Level: Medium

Description: Unauthorized individuals may follow authorized personnel into secure areas.

Recommendation: Implement a policy requiring employees to challenge unknown individuals, and conduct regular security awareness campaigns.

Lost or stolen devices:

Risk Level: High

Description: Mobile devices or laptops containing sensitive information may be lost or stolen.

Recommendation: Implement a policy requiring employees to report lost or stolen devices, and conduct regular security audits.

Unsecured disposal of sensitive materials:

Risk Level: Medium

Description: Sensitive documents or devices may not be properly disposed of.

Recommendation: Implement a policy requiring secure disposal of sensitive materials, and conduct regular security audits.

Inadequate surveillance:

Risk Level: Medium

Description: Lack of cameras or monitoring may make it difficult to detect and respond to physical threats.

Recommendation: Implement a surveillance system, and conduct regular security audits.

Poorly secured data centers:

DAY 7 {2}

Risk Level: High

Description: Data centers may not have adequate physical security measures in place.

Recommendation: Implement access controls, surveillance, and other physical security measures in data centers.

Inadequate access controls:

Risk Level: High

Description: Access controls may not be sufficient to prevent unauthorized access to sensitive areas.

Recommendation: Implement multi-factor authentication, and conduct regular security audits.

Operational Threats Vulnerabilities:

Insufficient patch management:

Risk Level: High

Description: Failure to keep software and systems up-to-date with security patches.

Recommendation: Implement a patch management process, and conduct regular security audits.

Inadequate change management:

Risk Level: Medium

Description: Changes to systems or processes may not be properly tested or documented.

Recommendation: Implement a change management process, and conduct regular security audits.

Lack of redundancy:

Risk Level: High

Description: Critical systems or processes may not have adequate redundancy or backup systems.

Recommendation: Implement redundancy and backup systems for critical systems and processes.

Inadequate incident response plan:

Risk Level: High

Description: The organization may not have a plan in place to respond to operational threats.

Recommendation: Develop and implement an incident response plan that includes procedures for responding to operational threats.