MARK JOHN RAMA JOPIA

BSIT – 2

IPT101

F-Seatwork Task 2

1. Summarize the PowerPoint presentation that is posted in the module: Lesson
    - Cybersecurity is crucial for protecting sensitive information and ensuring data integrity, using cybersecurity protection methods like firewalls, encryption, intrusion detection systems, and multi-factor authentication, guided by standards on cybersecurity such as ISO 27001 and NIST. Best practices in cyber protection methods include regular updates, employee training, strong password policies, and incident response planning, with information recovery relying on regular backups, disaster recovery plans, and continuous monitoring to quickly detect and respond to breaches.

2. Discuss the role of Advanced Persistent Threats (APT) in cyber espionage. How do APTs differ from other types of cyber-attacks, and what are the typical targets and objectives of APTs? Illustrate your answer with examples of known APT incidents.
    - Advanced Persistent Threats (APTs) are serious and targeted cyber-attacks often supported by governments. These attacks are designed to secretly get into important systems like those of defense contracts, finance, chemical industries manufacturing and IT services, and stay hidden for a long time to gather valuable information.

3. Evaluate the significance of standards and best practices in cybersecurity, such as those established by ISO and NIST. How do these standards help organizations mitigate risks associated with cyber-attacks? Include an analysis of the Plan-Do-Check-Act (PDCA) model and its application in implementing ISO 27001.
    - Standards and best practices in cybersecurity, like those from ISO and NIST, help organizations reduce risks from cyber-attacks by providing guidelines for managing information security, and the Plan-Do-Check-Act (PDCA) model within ISO 27001 ensures continuous improvement in security measures.

4. Examine the concept of social engineering in cybersecurity. What techniques are commonly used in social engineering attacks, and why are they often successful? Discuss the measures organizations can take to protect against social engineering attacks, using specific examples to support your points.
    - Social engineering involves manipulating people into sharing sensitive information or performing actions that compromise security, typically through tactics like phishing, pretexting, and baiting, exploiting human psychology and often succeeding due to the vulnerability of human error, but organizations can mitigate risks by educating employees, implementing strict security policies, and using measures like multi-factor authentication.