JEORGE ANDREI T. ELEVENCIONADO SEATWORK TASK 2

1. Summarize the PowerPoint presentation that is posted in the module:

**The "Cyber Security Standards and Best Practices" presentation highlights the importance of protecting systems and networks from cyber threats. It explains key cybersecurity standards like ISO 27001, the NIST Cybersecurity Framework, and CMMC, and stresses the need to follow these guidelines for strong security.**

**The presentation also covers easy-to-follow best practices, such as using strong passwords, regularly checking for security issues, keeping software updated, encrypting important data, and having plans in place for responding to security incidents and disasters. It explains how to handle security incidents by quickly identifying and managing them, informing the right people, analyzing what happened, and taking steps to prevent future problems. The presentation wraps up by encouraging organizations to adopt these practices to stay safe and keep their operations running smoothly**.

1. 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 complex cyber attacks that aim to sneak into and stay inside a network or system for a long time. These attacks are usually carried out by highly skilled groups like nation-states or organized crime. What makes APTs different from other attacks is their persistence, customization, stealth, and resourcefulness. They stay hidden in the target network, using various methods to avoid detection while they gather sensitive information, steal intellectual property, or disrupt important systems. APTs are specifically designed for their targets, using tactics like social engineering to get initial access and then deploying custom malware. They use advanced tools to remain undetected and adapt their methods as needed to achieve long-term goals like gaining strategic advantages or causing significant disruptions.**

**APTs often target government agencies, big corporations in sectors like technology, finance, or defense, research institutions, and essential infrastructure such as power grids and healthcare systems. Some well-known APT incidents include Stuxnet, which disrupted Iran's nuclear program; Operation Shady RAT, which stole sensitive information from many organizations; Operation Aurora, which attacked companies like Google and Yahoo!; and APT1, a Chinese group** **that targeted various organizations to steal information. In summary, APTs are highly sophisticated attacks that stay hidden and adapt over time to achieve long-term objectives by continuously exploiting targeted networks.**

1. 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.

**Cybersecurity standards and best practices from organizations like ISO and NIST are crucial for keeping systems and data safe. These standards give organizations a clear plan to manage and reduce risks from cyber-attacks and ensure they follow the law. By using ISO and NIST guidelines, organizations can better identify and handle cyber risks, lowering the chances and impacts of attacks. Following these standards also helps avoid legal issues and damage to reputation. Best practices include using strong passwords, regularly checking for security issues, assessing risks, and keeping software updated. The Plan-Do-Check-Act (PDCA) model in ISO 27001 supports ongoing improvement in cybersecurity by continuously planning, doing, checking, and acting on security measures.**

**To implement ISO 27001, organizations need to set up a system with policies and controls for cybersecurity. They must assess risks to find and address security threats. After setting up necessary controls, they regularly monitor and evaluate their effectiveness. Based on the findings, they take corrective actions and continuously improve by updating policies and providing more training. This ongoing process helps organizations maintain strong cybersecurity measures and stay compliant with regulations, effectively managing cyber risks and protecting their systems and data.**

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 is a type of cyber attack that tricks people into giving away access to systems, data, or sensitive information. These attacks use psychological tactics to fool individuals into revealing confidential information or taking actions that compromise security. Common methods include phishing (sending fake emails to get sensitive info), pretexting (making up stories to gain trust), baiting (leaving infected devices in public), whaling (targeting high-level executives), and quid pro quo (offering something in return for information). These attacks are effective because they take advantage of human weaknesses like trust and curiosity, and often target organizations with weak security.**

**To defend against social engineering attacks, organizations should train their employees regularly on cybersecurity practices and create a culture of security awareness. This helps employees recognize and resist these attacks. Strong monitoring systems can detect suspicious activities, and two-factor authentication adds extra security, making unauthorized access harder. Having a plan to respond to incidents quickly can limit the damage. Famous social engineering attacks include breaches at Target, Yahoo, and LinkedIn, where attackers used stolen login details and exploited system weaknesses. In summary, preventing social engineering attacks requires good training, awareness, strong security measures, and being prepared for incidents.**