Michael Joseph Melo
INF 225
04/30/2025

1. Explain why employees are considered both the strongest defense and the greatest risk in cybersecurity. Provide examples to support your answer.

- Employees are the strongest defense and the greatest risk in cybersecurity because they serve as the bridge and first line of defense between the cyber world and the organization. They are considered the organization's biggest asset and the most significant security liability at the same time. With threats becoming increasingly rampant, it only takes a single action by one employee to determine the safety and security of the entire organization. For example, employees may make mistakes that put the organization's data or system at risk. Such situations may occur due to carelessness, accidents, or lack of proper training in standard operating procedures and workplace protocols (*The Human Factor in IT Security*, n.d.). With proper training and the right decision-making, these accidents may not happen in the first place and can be further prevented. Following security protocols ensures the safety of the organization's sensitive information and maintains business operations.

2. Describe the role of Deep Learning and Artificial Intelligence in emerging cybersecurity technologies. How do they improve system security?

- As time goes by, digital transformation continues to advance. Some of the prominent products of technological advancements are deep learning and artificial intelligence. And, organizations are becoming increasingly aware of the benefits of these modern technologies offer. In the context of cybersecurity, artificial intelligence has proven to be a crucial asset in tackling cybersecurity concerns. It uses automated detection and analysis to help security systems manage large amounts of data and adapt to new threats (Legit Security, 2025). Artificial intelligence assists security professionals by recognizing complex data patterns. These modern approaches provide actionable recommendations and autonomous mitigation, addressing specific security challenges effectively.

3. Discuss the importance of the CIA Triad in cybersecurity. How does each element (Confidentiality, Integrity, and Availability) contribute to protecting data?

- The CIA triad (Confidentiality, Integrity, and Availability) serves as a foundational model for the development of security systems within an organization (Hashemi-Pour & Chai, 2023). These three principles ensure that sensitive data are protected from threats and businesses remain operational. Confidentiality refers to the authorized access to sensitive information. It ensures that information access is free from unauthorized use, allowing only individuals with proper authorization and privileges. On the other hand, integrity involves making sure that data is firm and free from tampering. An accurate and consistent information gains trust from the users, thus strengthening the credibility of an organization. It also affects the organization itself in a way that receiving incorrect information can lead to disastrous consequences. For example, if a hospital's system displays inaccurate patient records, it could result in misdiagnosis or improper treatment. And lastly, availability refers to data must be accessible to authorized users. Information should be accessible in times of need, ensuring that authorized users can retrieve it whenever necessary to perform their tasks effectively.

4. Imagine you are hired as a cybersecurity consultant for a company. What steps would you recommend they take to strengthen their cybersecurity processes?

- If I were hired as a cybersecurity consultant for a company, I would regularly conduct employee training regarding cybersecurity. As mentioned above, employees are the first line of defense in cybersecurity, playing a frontline role in protecting the organization from threats through their actions and awareness. Having regular training keeps employees up to date with the latest cybersecurity threats and best practices, ensuring they remain aware of new protocols and how to respond effectively to emerging risks. In addition, I would conduct risk assessments to further strengthen the cybersecurity processes. This serves as the first step in maintaining the security of the system. By identifying and evaluating the company's current condition, I would formulate an effective response to address existing risks and implement additional security measures to further enhance the overall cybersecurity posture. And lastly, I would implement a stronger access control to ensure that only authorized users have access to sensitive information, minimizing the risk of security breaches.

5. Explain how the supply chain can become a cybersecurity risk for a company. Suggest ways to protect against supply chain vulnerabilities.

- Supply chain can become a cybersecurity risk for a company due to multiple entities involved in the system. With more people involved, the higher the risk of human

error which can compromise the security and integrity of systems and data. Third-party entities may also have different security protocols from one another, therefore having different approaches or procedures in certain situations. Having sub-standard protocols serves as an entry point for cyberattacks and data breaches, risking the company entirely. One of the key considerations for cyber security in supply chain management is implementing robust risk management practices on each vendor. Vendors should comply with security standards to enhance network security measures and have regular assessment and update on security protocols to address threats (Etheridge, 2024). In addition, companies should consider vulnerability scans. Vulnerability scanning enables early detection of low-level vulnerabilities and access points to sensitive data. By identifying weaknesses early, vulnerability scanning also saves time and resources that would otherwise be spent responding to more severe incidents later on.

Reference:

Etheridge, E. (2024, September 16). *Cyber Security & Supply chain Risk Management: Mistakes & best practices*. DataGuard. https://www.dataguard.com/blog/cyber-security-and-supply-chain-risk-management/#:~:text=Key%20considerations%20for%20cyber%20security,assessing%20and%20updating%20security%20protocols

Hashemi-Pour, C., & Chai, W. (2023, December 21). *What is the CIA triad (confidentiality, integrity and availability)?* WhatIs. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Legit Security. (2025, March 20). *Understanding the role of AI in cybersecurity*. https://www.legitsecurity.com/aspm-knowledge-base/role-of-ai-in-cybersecurity#:~:text=Deep%20Learning&text=It's%20particularly%20useful%20for%20tasks,activities%20with%20minimal%20human%20oversight

*The human factor in IT security: how employees are making businesses vulnerable from within*. (n.d.). Kaspersky. https://www.kaspersky.com/blog/the-human-factor-in-it-security/