**Week2 Reflection on Cybersecurity**

Hang Yang

IS 5403: Cybersecurity

Prof. Jaime Martinez

March 23, 2024

**Week2 Reflection on Cybersecurity**

This week, we delved into fundamental aspects of cybersecurity and computing, including roles, processes, and an introduction to operating systems. Dr. McIver underscored the foundational significance of the CIA Triad in cybersecurity, highlighting the pivotal role individuals play in defense—an outlook I fully endorse. At its core, cybersecurity revolves around ensuring the confidentiality, integrity, and availability of data—an essential concern not just for businesses but also for our everyday lives. Consider personal information like banking details or medical records; confidentiality ensures that such sensitive data remains inaccessible to unauthorized individuals. Likewise, data integrity guarantees that information remains unaltered and reliable, crucial for activities like financial transactions where accuracy is paramount. Additionally, data availability ensures that essential services remain accessible without interruption, preventing scenarios like missed bill payments due to website crashes or account unavailability.

The staggering financial toll of cybercrime, as evidenced by the $10.3 billion reported in 2022 alone, underscores the urgency of safeguarding against cyber threats (Statista, 2024). Different roles entail varying responsibilities regarding cybersecurity, but its significance permeates our daily lives. It's imperative that everyone remains cognizant of this reality and takes proactive measures to safeguard themselves, their organizations, and public security. Dr. McIver rightly highlights the challenge of achieving all aspects of the CIA Triad simultaneously in today's rapidly evolving network landscape. Balancing user demands for enhanced experiences with the need for robust security measures often necessitates trade-offs, such as sacrificing some aspects of the Triad for immediate user gratification.

However, I respectfully diverge from Dr. McIver's stance on budget allocation in cybersecurity. While prioritizing the core functionality of products is undoubtedly crucial, modern distributed systems present challenges in delineating a clear "core." In such environments, comprehensive protection encompassing both core functionalities and peripheral layers is vital. Allocating resources to build a layered defense, from external safeguards to internal controls, is prudent. Moreover, investing in innovative cybersecurity solutions tailored to decentralized systems, such as XYZ solution, can effectively address the unique challenges posed by distributed architectures. By embracing a holistic approach to cybersecurity investment, organizations can better fortify themselves against the evolving threat landscape while sustaining operational efficiency and user satisfaction.

**References**

Chen, S., Wu, Z., & Christofides, P.D.(2021). Cyber-security of centralized, decentralized, and distributed control-detector architectures for nonlinear processes. Chemical Engineering Research and Design. Volume 165, January 2021, Pages 25-39. Retrieved from https://doi.org/10.1016/j.cherd.2020.10.014

not your CISO (2022, March 13). Cybersecurity in 2022: What to Focus on. Medium. Retrieved from https://medium.com/dark-roast-security/cybersecurity-in-2022-what-to-focus-on-16ef41de76b9