Collaborative Learning Discussion 1

Summary Post

I'd like to use this time to express my appreciation for everyone's perspectives, ideas, facts, and concerns about cybersecurity. I stand by my assertion that e-commerce and related businesses are the primary targets of cyber attacks. After COVID19 lockdowns, digital platforms, work-from-home opportunities, and internet purchasing all reached new heights. As I indicated in my initial post, firms should begin investing in areas such as strong secure solid IT infrastructure, mitigating cyber attacks and cyber crime forensics with legal actions as a part of their future digital well-being.

I appreciate my peer Sahib Jabbal's addition of a critical point about the need of digital payment channels and user awareness. Another significant reaction, this time from my peer Abraham Gordon, has raised his concerns about the dangers of remote employment. I agree with his assertion that when remote work is secure and optimized by design, including processes, guidelines, and standards, the only remaining risks should be those associated with the zero-day vulnerabilities and obsolescence. “Digital freedom stops where that of users begins.. Nowadays, digital evolution must no longer be offered to a customer in trade-off between privacy and security. Privacy is not for sale, it's a valuable asset to protect.” by Stephane Nappo is the Global Head Information Security for Société Générale International Banking.

Additionally to the aforementioned arguments, Unit1-3 chapters in our Cyber security course have elevated my viewpoints. Beginning with the most prevalent types of cyberattacks, the PPDR, the CIA Triangle, the metadata level, the importance of GDPR (General Data Protection Regulations), and legal acts, this session got off to a fantastic start. Fundamentals of networking and database systems provided a solid foundation for this program. Password eavesdropping concerns, encryption approaches, man-in-the-middle attacks, and multiple authentication factors all aid me in my day-to-day digital life. The chapter on network assault and defense has re-energized my networking thoughts. After completing these units, I am convinced that I will play a critical role in our continuous fight to combat cybercrime and address security concerns.

References:

"Impact of COVID-19 on digital platforms and change in E-commerce shopping trends" Bhavna Galhotra and Ayushi Dewan. Proceedings of the Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) IEEE Xplore Part Number:CFP20OSV-ART.

"E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal" Lawrence J. Trautman 16 U.C. Davis Bus. L.J. 261 (2015-2016).

"k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities" by Lingyu Wang; Sushil Jajodia; Anoop Singhal; Pengsu Cheng; Steven

Noel; Published in: IEEE Transactions on Dependable and Secure Computing (Volume: 11, Issue: 1, Jan.-Feb. 2014) Page(s): 30 - 44.

"Computer Science: An Overview, Global Edition" by Glenn Brookshear and Dennis Brylow; 13th ed. Addison Wesley Longman Inc. Chapter 4 and 9.

"Security Engineering - A Guide to Building Dependable Distributed Systems" 3rd Edition by Ross Anderson; Published by John Wiley & Sons, Inc., Chapter 2,4,15 and 21.