Summary Post – Cyber Security as a global Issue

In the initial post, I stated that cyber threats would continue to be on the front burner as long as individuals, businesses and government continue to use data (VanSyckel, 2018). This underscores the importance of cyber security at all levels of human existence globally. It is therefore imperative that individuals, businesses and government invest appropriately and adequately in cyber security. Otherwise personal identity, company competitiveness and national election among other important things could be undermined by cyber attacks. The global impact of a cyber attack could be gleaned from the recent attacks on the oil industry. In February 2022, major oil terminals in Western Europe were hacked (Centre for Strategic and International Studies, 2022). The incident disrupted the unloading of barges resulting in down time, financial losses and strain on the availability of petroleum products around Europe.

Furthermore, the Yahoo data breach in December 2014 showed that when one online account is breached, it frequently leads to the breach of other accounts linked to the targeted user (National Law Review, 2018). This kind of breach is made possible because users share credentials among accounts without the application of multi-factor authentication. Similarly, data breaches could be prevented at the design stage of a system by the use of a threat model like the STRIDE, which can be used to identify and eliminate potential vulnerabilities before a single line of code is written (Hewko, 2021). Accordingly, using threat modeling techniques should be the starting point for designers of networks, systems, and applications. Additionally, regulatory compliance improves operational efficiency, reduces legal problems and

fosters customers' trust. The General Data Protection Regulation (GDPR), for example, affects data privacy and encourages businesses to build cyber security systems that can mitigate the dangers of a data breach.

Although there may be some added challenges to overcome when it comes to integrating security, it is a critical issue that should be prioritized.

References

British Broadcasting Corporation. (2021). *Cyber attack on Irish health service 'catastrophic'*. Available from https://www.bbc.com/news/world-europe-57184977 [Assessed 25 March 2022].

Centre for Strategic and International Studies. (2022). *Significant Cyber Incidents*. Available from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Assessed 25 March 2022].

Hewko, A. (2021). *STRIDE Threat Modeling: What You Need to Know*. Availablr from https://www.softwaresecured.com/stride-threat-modeling/ [Assessed 25 March 2022].

National Law Review. (2018). *The Hacked and the Hacker-for-Hire: Lessons from the Yahoo Data Breaches*. Available from https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far [Assessed 25 March 2022].

Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems , 92*, 178-188.

VanSyckel, L. (2018). *Sealevel Systems White Paper - Introducing Cybersecurity*. Available https://www.sealevel.com/support/white-paper-introducing-cybersecurity/ [Assessed 25 March 2022].