Summary of the Discussion on Why Cyber Security Is Now a Global Issue and Why it is Important for Companies to Invest in It

In accordance with my initial post and an illuminating discussion with my peers, it is clear that cybersecurity is a global issue due to more businesses and people embracing technology by performing most of their operations digitally (especially now due to the Covid-19 pandemic).

Moreover, usage of IoT devices for sensitive data like governmental operations, healthcare, banking, etc, has automatically led to cybercriminals targeting them and gaining easy access to most of these devices.

Such attacks include: Viruses, Malwares like ransomwares, Denial of Services, Phishing, etc. (VanSyckel, 2018)

Additionally, I got to have a better understanding on how important it is for companies to invest in cybersecurity. Indeed, businesses with a higher level of cyber-security will have a competitive advantage and credibility in the market seeing that their clients will trust them more with processing and handling of their personal information. Not forgetting the financial benefits, whereby, issues like: industrial espionage (as mentioned in Marios' post), covering of damage costs like ransomware, and exposure to regulatory actions like additional tax compliances, penalties, etc, would be avoidable if a system is secure from attacks (Vaidya, 2019). I also found Patricia's video on Kevin Mitnick been an eye-opener.

As from the first 3 units' contents of this module, it shows how cybersecurity professionals have the skills to advise and apply reliable preventive, detection and

response measures and technologies on systems, networks and devices, so as to deal with cyberattacks.

Such measures and technologies may include:

- Setting up security protocols like passwords, cryptography, data encryptions, internet protocol, etc, that governs communication in system(s). (Anderson, 2020).
- Abiding to ethical and legal responsibilities like data protection, data confidentiality and privacy and also the C.I.A. triangle of cybersecurity i.e., Confidentiality, Integrity and Availability.
- Using VPNs, firewalls, cryptography, endpoint security antiviruses, control measures, doing threat risk assessment and penetration tests to systems and networks so as to patch up the vulnerabilities. (CyBOK, 2021).
- Plus, the need of businesses to get security insurances, and training of employees on cybersecurity and General Data Protection Regulation (GDPR) awareness since most breaches are due to human errors, and also encouraging users to report on the errors and attacks.

References

Anderson, R., 2020. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3rd ed. Indianapolis, USA: Wiley.

CyBOK, 2021. *Knowledgebase1_1.* [Online]

Available at: https://www.cybok.org/knowledgebase1_1/

[Accessed 27 March 2022].

Vaidya, R., 2019. *Cyber Security Breaches Survey 2019.* [Online]

Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf

[Accessed 16 March 2022].

VanSyckel, L., 2018. *White Paper: Introducing Cybersecurity.* [Online]

Available at: https://www.sealevel.com/support/white-paper-introducing-cybersecurity/

[Accessed 26 February 2022].