Summary Post

Thanks for the contributions and reviews made by Austin, M, Zihaad, K, Aldo, M, Haseeb, A and Kingsley, O. Here is my summary below.

Summary

In conclusion, based on the initial post and the feedback from peers, further proof that cyber-threats can impact on a planetary-scale as well as a global issue now. The cyber threats are unexpected and often results in huge substantial financial or reputation loss, therefore it is important for companies to invest to prevent it.

According to the Cyber Security Breaches Survey of 2021 (Department for Digital, Culture, Media and Sport, 2021), reflected a positive impact on cyber security in the UK with the GDPR legal framework. Although there were some downsides in short term like increased cyber risk by concealing personal information from ICANN and WHOIS (Kevin, R., 2020), forcing organisations not limited in European Union to incorporate better cyber security policy and strategy can reduce the impact of cyber threats and even avoid being victims of cyberattacks in long term. Every country should focus on catching up on cybercrime and reviewing its policy.

Invest in Cyber Security is not only consumable, but also it is a kind of advertisement. The organization advertises in data security and privacy have gained a competitive advantage now a day. Encrypted messenger like Wire, gained enormous popularity owing to their simplicity and focus on data privacy with their concept of “security by design”. (Bernardo, A., 2021)

Under the COVID-19 stretching, direct monitoring from organisations has become more difficult where staff are working remotely. On the one hand, companies should be aware of the new challenges in security breaches and attacks when investing in new technology. On the other hand, the remote work trend motivated organisations to upgrade systems and decommission the end-of-life system which prevents and reduces vulnerabilities impact.

Finally, the use of human psychological weaknesses attacks like phishing was the most common and disruptive cyber-attack in support of the survey in 2021 (Department for Digital, Culture, Media and Sport, 2021). Therefore, besides of the invest in hardware and system, companies invest should focus on staff training to avoid human factors. “Only amateurs attack machines; professionals target people.” (Bruce, S, 2000).

References:

Department for Digital, Culture, Media and Sport. (2021) *Cyber Security Breaches Survey 2021: Statistical Release*. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/972399/Cyber\_Security\_Breaches\_Survey\_2021\_Statistical\_Release.pdf [Accessed 30 August 2021].

Kevin, R. (March 24, 2020) GDPR and WHOIS: Here's What You Need to Know. *Cisco Umbrella*. Available from: https://umbrella.cisco.com/blog/gdpr-and-whois [Accessed 30 August 2021].

Bernardo, A. (January 22, 2021) The desire for a secure messenger environment is only likely to keep growing. *EU Startups.* Available from: https://wire.com/en/blog/the-desire-for-a-secure-messenger-environment-is-only-likely-to-keep-growing [Accessed 30 August 2021].

Bruce, S. (October 15, 2000) Semantic Attacks: The Third Wave of Network Attacks, 2000-10-15. *Schneier on Security*. Available from: https://www.schneier.com/crypto-gram/archives/2000/1015.html#1 [Accessed 30 August 2021].