Summary Post
Monday, 28 March 2022, 11:33 PM

I agree with most posts of my peers about the treats that the world is currently facing regarding cybersecurity as a global issue. The digital transformation that world is currently experiencing has brought many benefits such keeping businesses, people and many more connected. However, the adoption of all these new technologies came with unprecedented treats that the world has never faced before which cyber criminality and the treat is particularly damaging for companies.

According to the Cybersecurity Ventures (2017), "*cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind".* The article continues by pointing out how the damages caused by cyber criminals cost nearly $3 trillion in 2015 and the number will only increase. These cyber-attacks are you usually carried out using virus, malware, phishing, denial of service trojan horse, worm, and many more (Brookshear, Brookshear, and Brylow, 2019).

As stated above the world is moving on the digital direction, we shop online, banking transaction are mostly done online nowadays, the development of new technologies which yet to be fully adopted such AI, 5G etc… all this required organisations to collect data from the public. So, when an organisation is breached by cyber criminals with the sole intent to access this type information for bad purposes, this can cause a reputational damage, revenue losses and many more to the organisation. Just because of this risk cybersecurity solution should be at the top of businesses agenda (Lee, Zankl and Chang, 2016). Although there are regulations in place to protect the public against privacy such as Data Protection Directive 95/46/EC and the General Data Protection Regulation (GDPR), the US Federal Trade Commission's Fair Information Practices and more, but this don't discourage cyber criminals to commit illegal activity and businesses to have poor cybersecurity culture.

Companies should design secure systems to protect themselves against cyber-attacks such as having various of types of firewall in place. Al a global issue and why it is important for companies to invest in Cyber Security so companies' various approach in place to identify attacks such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege.

In summary we can agree that a global issue and why it is important for companies to invest in Cyber Security

Brookshear, G., Brookshear, J. and Brylow, D. (2019). Computer Science: An Overview, Global Edition. 13th Edition. [UK]: Pearson International Content.

Morgan, S (2017) Cybercrime Damages $6 Trillion By 2021, Available at: **https://cybersecurityventures.com/annual-cybercrime-report-2017/#:~:text=Cybersecurity%20Ventures%20predicts%20cybercrime%20damages,in%20size%2C%20sophistication%20and%20cost** (Accessed: 23/03/2022).

Department for Digital, Culture, Media & Sport (2020) Cyber Security Breaches Survey 2020, Available at: **https://www.gov.uk/government/statistics/cyber-**

security-breaches-survey-2020/cyber-security-breaches-survey-2020 (Accessed: 23/03/2022).

Lee, W., Zankl, W. and Chang, H. (2016). *An Ethical Approach to Data Privacy Protection*. www.isaca.org. Available at: **https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection**. (Accessed: 23/03/2022).