Due to various great contributions from fellow students enhancing my initial post, the question why Cyber Security is now a global issue and why it is important to invest in Cyber Security could be thoroughly elaborated.

Discussing a medical device company helped to point out, that fines imposed by regulations such as HIPAA and GDPR are a strong motivator to invest in Cyber Security for companies in general. This is because fines are in the millions of Euros and therefore can even hurt the biggest companies regardless of the sector they are operating in (Ritzar and Filkina, 2019), (Alder 2021). During the discussion it was also identified, that Artificial Intelligence (AI) as a new technology might tempt companies to retain data to train their algorithms. This however can be in violation with a regulation such as GDPR, where data of an individuum may only be kept for a limited time. An attack revealing such data was leaked, would likely to result in fines not only for insecure storage but additionally also for data processing beyond its permissible purpose (GDPR 2016).

Additionally it was argued, that AI also might be used to attack in the future, since AI is likely to develop smart algorithms, that will be very dynamic and hard to anticipate (Tschider 2018). Building up a defence to such a threat scenario will be challenging and according to Creese et al. (2020) a global approach is necessary to develop effective tools to defend.

Ironically AI could on the other hand also be used to prevent attacks from happening by monitoring relevant big data generated within a company such as e.g. traffic. AI could be able to monitor the traffic of a large cooperation and could identify patterns, that could point to the fact that e.g. account credentials are abused (Budek 2020).

During the debate it was agreed, that skipping cyber security is only beneficial for some companies (Williams 2019). In particular it might only be good for companies, that need to provide evidence fast, that their business model will generate revenue. For the majority of companies however it is more beneficial to invest in cyber security from the beginning. For a medical device company in particular, it was argued, that loss of availability and integrity might lead to harm of patients, which makes cyber security a topic that cannot be skipped. (Pesapane et al. 2108)

That quantum computing will render current encryption ineffective was not in dispute, but quantum computing still needs some time to be broadly available (Lichfield 2020)(Stolbikova 2016). AI on the other hand was seen as a technology that can shift the threat landscape in the near future to a very dynamic scenario.

In conclusion it can be stated, that AI and hefty fines imposed by regulations can be seen as strong motivators for companies to now invest in cyber security.

References

Alder, S. (2021) *What are the Penalties for HIPAA Violations?* Available at: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [Accessed 12.02.2021]

Budek, K. (2020) *AIOps Network Traffic Analysis (NTA) – a business guide*. Available from: https://deepsense.ai/aiops-network-traffic-analysis-nta-a-business-guide/ [Accessed 13.02.2021]

Creese, S. et al. (2020) *Future Series: Cybersecurity, emerging technology and systemic risk INSIGHT REPORT NOVEMBER 2020*. Available from:

http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf [Accessed 27.01.2021]

GDPR (2016) *REGULATION (EU) 2016/679*. Available from: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 [Accessed 13.02.2021]

Lichfield, G. (2020) *Quantum supremacy*. Available from: https://www.technologyreview.com/technology/quantum-supremacy/ April 2, 2020 [Accessed: 12.02.2021]

Pesapane, F., Volonté, C., Codari, M. & Sardanelli, F. (2018) *Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights Imaging*. 9:745–753. Available from: https://doi.org/10.1007/s13244-018-0645-y [Accessed: 12.02.2021]

Ritzar, C and Filkina N (2019) *Data Protection Report*. Available from: https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/ [Accessed: 12.02.2021]

Stolbikova, V. (2016) *Can Elliptic Curve Cryptography be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem*. Available from: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/can-elliptic-curve-cryptography-be-trusted-a-brief-analysis-of-the-security-of-a-popular-cryptosyste [Accessed: 12.02.2021]

Tschider, C. (2018) *Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*. 5 Savannah L. Rev. 177. Available from: https://ssrn.com/abstract=3070000 [Accessed: 12.02.2021]

Williams, L. et al. (2019) *Secure Software Lifecycle Knowledge Area Issue 1.0*. Crown. Available from: https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_issue_1.0.pdf [Accessed 26.01.2021]