Collaborative Discussion 1: Digitalisation – What are the security implications of the digital economy?

My Initial Post:

According to Wei et al. (2019), digital utilities can benefit significantly from optimising processes, understanding customers, empowering employees, enhancing security, and reducing risks. Siemens (N.D.) suggests that a "fully digital enterprise" relies on digital tools and technologies for its operations, utilising digitised assets and resources. Cyber-physical systems, cloud computing, IoT, AI, and machine learning are employed to automate processes and improve efficiency, quality, and time.

As technology advances, new vulnerabilities arise, and it's crucial to implement efficient controls to detect and prevent complex cyber threats (Spremić & Šimunic, 2018). According to Shea (2023), cybersecurity requires a collective effort from the entire organisation, as cyber threats like data breaches, ransomware, and supply chain attacks pose significant business risks.

Brick-and-mortar stores struggle with web-based retailers due to higher costs. Some have adapted by creating online (Murphy, 2022). These SMEs face significant cybersecurity challenges due to remote work and growing cyber threats. Their competitiveness and value chain can be seriously impacted by low-security budgets, a lack of cyber skills, and increased cyber-attacks (ENISA, N.D.).

I agree with the viewpoints expressed in the articles. The IEA's (2022) report on the energy crisis emphasised the importance of reducing business's dependence on fossil fuels. A fully digital enterprise can achieve these goals by reducing energy consumption, improving efficiency, and adapting to changing circumstances.

References:

- Wei, J., Sanborn, S., Slaughter, A. (2019). *Digital transformation and the utility of the future | Deloitte Insights*. [online] Available at: https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/digital-transformation-utility-of-the-future.html.
- Siemens (N.D.). *Digital Enterprise | Siemens*. [online] Available at: https://www.plm.automation.siemens.com/global/en/our-story/glossary/digital-enterprise/25213.
- Spremić, M. & Šimunic, A. (2018). *Cyber Security Challenges in Digital Economy*. Available at: https://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf
- Shea, S. (2023). *Top 7 enterprise cybersecurity challenges in 2022*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/tip/Cybersecurity-challenges-and-how-to-address-them.
- Murphy, C. (2022). *How Brick And Mortar Stores are Performing and Adapting*. [online] Investopedia. Available at: https://www.investopedia.com/terms/b/brickandmortar.asp.
- ENISA (N.D.). *SME Cybersecurity*. [online] Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity.
- IEA (2022). *Executive Summary – World Energy Outlook 2022 – Analysis*. [online] IEA. Available at: https://www.iea.org/reports/world-energy-outlook-2022/executive-summary.