Module 3 - Network Security - Collaborative discussion 1
Unit 1 - “INITIAL POST”

Fully digital enterprise

A fully digital enterprise could be an organization or business which has fully transitioned into a digital economy. A digital economy being a business or service which is based on integration of technologies as a basic business infrastructure (*Read Wei et al. 2019*) .
According to (Oswald & Kleinemeier, 2017:ix), a digital economy has five defining trends. These five trends consist of supercomputing (Big data), Hyper-connectivity (IoT), Cloud computing, Smarter world (AI, ML, Robotics) and finally, Cyber Security (Oswald & Kleinemeier, 2017:ix).
For the majority of businesses, digitalization has become imperative and is no longer a choice (Oswald & Kleinemeier, 2017:3) if a company wishes to survive.

Cyber security challenges/concerns with a fully digital enterprise?

The cybersecurity challenges that companies may experience while adopting digitization via a Digital transformation with the aim of becoming a fully digital enterprise is on the rise. A survey carried out by Wei et al. (2019) showed that 41% of those surveyed had said that the threat of a cyber attack on their business is one of the forces that is impacting power companies the most.

Fully digital enterprises face many challenges related to the threat of a cyber attack taking place. Larger organizations may also be more difficult to defend during transition due to reasons such as system integration and complex systems. Organizations may have Operational technology with legacy applications running or hybrid Information technology architecture of on-premise data centers and cloud infrastructure. Digitalization of the business may expose many vulnerabilities which can be exploited by adversaries. These threats increase the financial expenditure (Wei et al. 2019) which is required to defend the digital footprint and systems within the businesses digital economy.

Cyber security challenges for a brick and mortar SME wanting to become a digital enterprise?

According to Spremić & Šimunic (2018) the main focus of cybersecurity is to design and implement effective controls. This could be performed by implementing an information security management system via the ISO27001 standard (ISO, 2023), to ensure that compliance, policies and procedures are maintained while enforcing confidentiality, integrity and availability of data and systems.

With a shortage of skilled staff available, finding and attracting competent individuals will be a challenge (Willmott, 2013; Mohamed, 2018) and a concern for businesses, especially for SMEs who may also have a lower budget than larger enterprises and may have many employees who are non-technical and require upskilling to carry out basic computer tasks. SMEs business models who are transitioning to industry 4.0, have an element called Competence risk (Kovaite & Stankeviciene, 2019). The competence risk can be used to highlight the possibility of a cyber

security incident taking place due to having non-competent employees or staff who are expected to operate the new digital systems within a traditional brick and mortar business.

Conclusion

To conclude, I think that both the fully digitalized enterprises and the brick and mortar SME would be susceptible to cybersecurity threats but for different reasons. The SMEs who wish to implement a digital transformation may be susceptible due to a lack of training/competence, a lack of financial means to employ proficient IT and cybersecurity teams with the auditing ability to implement competent controls and possibly a weak or exposed network and systems with no endpoint detection or incident response staff. Those businesses which have already transitioned may have a larger attack surface and various connected systems. The larger surface could statistically provide more points of entry or data leakage. But the digitalized business may have a higher level of technological competence, therefore, reducing risk and having a faster response time to incidents.

References

Deloitte 2018

ISO. (2023) ISO/IEC 27001. Available from: https://www.iso.org/isoiec-27001-information-security.html [Accessed on 27 January 2023].

Krovaite, K. & Stankeviciene, J. (2019) Risk of Digitalisation of Business Models. In: International Scientific Conference. Vilnius, Lithuania: VGTU Press, 380-387

Mohamed, M. (2018) Challenges and Benefits of Industry 4.0: An overview. International Journal of Supply and Operations Management. 5(3): 256-265

Oswald & Kleinemeier (2017) Shaping the digital enterprise. *Cham: Springer International Publishing*.

Wei et al. (2019) *Digital Innovation*. *Creating the utility of the future*. Deloitte Insights. Available from: [Accessed 26 january 2023].

Spremić, M. and Šimunic, A., 2018, July. Cyber security challenges in digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.

Willmott, P (2013) McKinsey Digital. The Digital enterprise. Available from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-digital-enterprise