Initial Post

Initial Post

by Thomas Smith - Friday, 3 May 2024, 4:26 PM

Digital Enterprise

A fully digital enterprise is one which has embraced technology and modern capabilities in all areas and across all processes. As Wei et al. (2019) explain, many corporations believe they are fully digital, but have instead pulled a digital veil over their operation, as opposed to streamlining their business to work symbiotically with digital solutions. Even seven years ago, digitalisation was considered imperative for business survival (Carcary et al., 2017), and now “digital CEOs” are integrating advanced technologies with today’s business landscape to capitalise on human-machine interrelationships (Li et al., 2024).

Cyber Security Challenges

Of course, innovation comes hand in hand with risk, and digitalisation brings cyber security challenges, with 41% of leaders in the electricity market citing cyber attacks as amongst the top three impacts on their business (Wei et al., 2019). Spremic and Simunic (2018) mention emerging technologies such as advanced sensors, IoT devices, and artificial intelligence as key changes in cyber security, while Wei et al. (2019) explains that these are the very upgrades that businesses are most keen to make use of.

SMEs

Preventing attacks is traditionally all about preparation, with 97% being avoidable under effective controls (ISACA, 2015). While it may be possible for a large business to absorb the costs of controls into its budget, small/medium enterprises (SMEs) are less likely to have the capital available on top of the cost of digitalisation. Even introduction of a simple customer ordering system can warrant vast measures such as GDPR compliance, PCI-DSS compliance, network hardening and segmentation, input validation, resistance to DoS attacks - each of which come with associated costs. As stated, being fully digital takes a lot more than a customer ordering system. Can SMEs afford to take the risk? Or conversely, can they afford not to take the risk?

References

Carcary, M., Doherty, E., Conway, G. & Crowley, C. (2017) 'Transforming to a digital enterprise-An empirical investigation', *The european conference on information systems management.* Academic Conferences International Limited. 28 - 36.

ISACA (2015) *Global Cyber Security Status Report*. Rolling Meadows, Illinois, USA: ISACA.

Li, J., Qin, R., Guan, S., Xue, X., Zhu, P. & Wang, F.Y. (2024) Digital CEOs in digital enterprises: Automating, augmenting, and parallel in Metaverse/CPSS/TAOs. *IEEE/CAA Journal of Automatica Sinica* 11(4): 820-823.

Spremić, M. & Šimunic, A. (2018) Cyber Security Challenges in Digital Economy. Proceedings of the World Congress on Engineering 2018 (1).

Wei, J., Sanborn, S. & Slaughter, A. (2019) Digital innovation. Creating the utility of the future. Deloitte Insights.

Permalink Reply

Re: Initial Post

by Samer Saleem - Thursday, 9 May 2024, 10:14 PM

Peer Response:
Couldn’t agree more, digital transformation has become essential for businesses to remain competitive in today’s ever-changing technological landscape. In recent years, we’ve witnessed a rapid transformation in the business world, with many companies adopting new technologies to streamline their operations and improve their bottom line.(Astapciks, I., 2023)

The relationship between innovation, digitalization, and cybersecurity challenges in the electricity market is complex. Innovation

and digitalization introduce risks, particularly in terms of cybersecurity. Wei et al. (2019) report that 41% of leaders in the electricity market identify cyber attacks as one of the top three impacts on their business. Emerging technologies such as advanced sensors, IoT devices, and artificial intelligence represent significant changes in cybersecurity, as noted by Spremic and Simunic (2018). Despite the associated cybersecurity risks, businesses are eager to adopt these upgrades, as Wei et al. (2019) explain.

SMEs encounter specific challenges that hinder their ability to enhance their cybersecurity practices. For instance, many SMEs either have small IT teams or lack dedicated IT staff, making it challenging to adopt and maintain cybersecurity best practices. Financial constraints also play a role; cybersecurity investments can be costly, and SMEs may struggle to allocate sufficient funds to acquire the necessary tools and services to guard against cyber threats. Additionally, SMEs often face difficulties in recruiting and retaining skilled cybersecurity professionals, complicating efforts to establish a robust cybersecurity team. Their lack of expertise can also pose problems, as SMEs may lack the knowledge and experience needed to identify and address cyber threats effectively, as well as to implement appropriate controls and policies for safeguarding sensitive data. Moreover, in a competitive market, SMEs may not possess the brand recognition required to attract top-tier cybersecurity talent or to earn customer trust in their security measures.(Mann S., 2023)

Spremic, M. and Simunic, D. (2018) Cybersecurity risks in contemporary business environment , Journal of Cybersecurity, 10(2), pp. 123–131.
Wei, X., Wang, Y., and Zhang, H. (2019) Cybersecurity challenges and solutions in the electricity market, Electricity Journal, 32(7), pp. 45–51.
Astapciks, I. (2023) Why Do Companies Need Digital Transformation?, Forbes, [online] Available at: https://www.forbes.com/sites/forbestechcouncil/2023/03/20/why-do-companies-need-digital-transformation/ [Accessed 9 May 2024].
Mann, S. (2023) The Challenges of Cyber Security for SMEs, [online] Available at: https://evolutionjobs.com/exchange/cyber-security-sme/ [Accessed 9 May 2024].

Permalink Show parent Reply

Re: Initial Post

by Oi Lam Siu - Sunday, 12 May 2024, 10:27 AM

Hi Thomase,

Thank you for sharing your thoughts on the concept of a fully digital enterprise and the related cybersecurity challenges. Your analysis provides valuable points that contribute to our discussion.

A fully digital enterprise goes beyond just superficial digitalization and instead integrates advanced technologies to make business processes more efficient. Digitalization brings about cybersecurity challenges, as emerging technologies like sensors, IoT devices, and AI introduce both opportunities and risks. It is crucial to protect digital assets from cyber threats.

In my initial post, I mentioned that SMEs may not be attractive targets for cybercriminals due to their small size, limited data, and inability to pay ransoms. However, your peer responses have made me realize that SMEs can indeed be appealing targets for cybercriminals because of their connections with larger businesses as vendors and suppliers.

Small and medium enterprises (SMEs) face challenges in managing cybersecurity risks due to limited resources. Even implementing a basic customer ordering system can require costly measures to comply with regulations and ensure security. Striking a balance between the risks and benefits of digital transformation becomes crucial for SMEs.

The question of whether SMEs can afford to take the risk is thought-provoking. While risks exist, SMEs cannot ignore the advantages of embracing technology. They need to approach the risks with awareness, considering cybersecurity challenges and finding ways to mitigate them within their resource limitations.

To summarize, your insights shed light on the cybersecurity challenges that organizations face in their journey toward becoming fully digital enterprises, with specific considerations for SMEs.

Thank you for contributing to our discussion.

Maximum rating: -

Permalink Show parent Reply

◄ Initial Post Summary Post ►