In contemplating a fully digital enterprise, Wei et al. (2019) illustrate a compelling vision where digital technologies like AI, IoT, and blockchain transform the power and utilities sector. Such an enterprise operates on real-time data analytics, advanced automation, and seamless integration across all of its operations. The future power company, as depicted, exemplifies this vision with its real-time situational awareness and smart home platforms. This transformation, however, brings significant cyber security challenges.

Spremic and Simunic (2018) emphasize that as organizations digitize, they become more susceptible to sophisticated cyber threats. A fully digital enterprise faces challenges such as protecting vast amounts of data, ensuring secure communication across interconnected systems, and safeguarding against advanced persistent threats (APTs).

For bricks-and-mortar SMEs transitioning to digital enterprises, the cyber security landscape becomes even more complex (Saeed et al, 2023). These businesses often lack the resources and expertise of larger corporations, making them more vulnerable to cyber attacks. Their challenges include securing legacy systems, managing increased cyber threat surfaces, and complying with evolving regulatory requirements. Implementing advanced security measures and fostering a cyber-aware culture are two measures that can help in mitigating these risks.

Reflecting on the views expressed, especially in light of the 2022 global energy crisis (Ozili & Ozen, 2023), the need for robust cyber security becomes even more apparent. The energy crisis underscored the fragility of critical infrastructures and the potential for cyber attacks to exacerbate such vulnerabilities. Wei et al.'s vision of digital innovation in the power sector must be coupled with Spremic and Simunic's call for advanced cyber security strategies to ensure resilience and sustainability.

To manage and mitigate these threats, organizations must adopt a multi-layered security approach. This includes deploying AI-driven threat detection systems, implementing strict access controls, and conducting regular security audits. Legal, social, ethical, and professional considerations also play a pivotal role. Information security professionals must navigate regulatory landscapes, protect user privacy, and maintain ethical standards while addressing cyber threats.

In summary, transitioning to a fully digital enterprise necessitates robust cyber security strategies to safeguard against emerging threats. The convergence of digital innovation and comprehensive security governance is essential for ensuring the resilience and sustainability of modern enterprises in an increasingly connected world.

REFERENCES

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

Spremić, M. and Šimunic, A. (2018) 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.

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), p.6666.

Ozili, P.K. and Ozen, E., 2023. Global energy crisis: impact on the global economy. The impact of climate change and sustainability standards on the insurance market, pp.439-454.