Initial Post

Display replies in nested form	Settings ⌄

Initial Post

by <u>Lauren Pechey</u> - Saturday, 21 June 2025, 1:19 PM

1. What do you consider a fully digital enterprise?

A fully digital enterprise is an organisation that uses digital technologies across all its operations, decision-making, and customer interactions. It includes cloud computing, artificial intelligence (AI), big data analytics, the Internet of Things (IoT), and automation tools to improve efficiency and competitiveness. Doroiman and Sîrghi (2024) found that higher levels of digital maturity, as measured by the Digital Economy and Society Index (DESI), positively relate to more innovation and economic growth in the European Union. A fully digital enterprise does not just use digital tools in isolated areas; it integrates them into its strategic and operational structure (Doroiman and Sîrghi, 2024).

2. What are the cybersecurity challenges or concerns for a fully digital enterprise?

While digital transformation brings many benefits, it also raises significant cybersecurity issues. Fully digital enterprises encounter a wide range of threats, including ransomware, phishing, data breaches, and supply chain vulnerabilities (Arshad & Azzam, 2023). As organisations depend more on cloud services, mobile workforces, and interconnected systems, their risk increases significantly as they now have to protect their expanding online presence (Arshad & Azzam, 2023). Doroiman and Sîrghi (2024) stress the need for strong security systems to go along with digital growth. In addition, following data protection laws like the General Data Protection Regulation (GDPR) creates legal and technical challenges (Voigt & von dem Bussche, 2017). Therefore, companies must balance digital innovation with a proactive cybersecurity plan.

3. What are the cyber security challenges for a bricks-and-mortar SME wanting to become a digital enterprise?

For small and medium-sized enterprises (SMEs) moving from traditional to digital models, cybersecurity presents specific challenges. These businesses often lack the technical skills and financial resources needed to put in place thorough security measures (Karim, Gide & Sandu, 2018). Common weaknesses include weak access controls, outdated systems, and insufficient employee training (Arshad & Azzam, 2023). Furthermore, SMEs are common targets for cyberattacks because of these issues. The digital transformation of these organisations should include strategic investments in scalable cybersecurity solutions, staff training, and risk management practices (Doroiman & Sîrghi, 2024). Not addressing these challenges can lead to data loss, damage to reputation, and legal consequences, ultimately slowing down successful digital adoption.

References:

Arshad, M. A., & Azzam, M. K. (2023) Success factors in traditional, digital, and hybrid startups of micro, small, and medium-sized enterprises in the retail industry. *International Journal of Academic Research in Business and Social Sciences* 13(12): 2728-2751. Available from: **https://www.researchgate.net/publication/376844460_Success_Factors_in_Traditional_Digital_and_Hybrid_Startups_of_Micro_Small_and_Medium-Sized_Enterprises_in_the_Retail_Industry** [Accessed 21 June 2025].

Doroiman, M.M. & Sîrghi, N. (2024) The Digital Enterprise Landscape: How DESI Metrics Shape Economic Growth in the EU. *Oradea Journal of Business and Economics*, 9(2), pp. 36–46.

Karim, F., Gide, E. & Sandu, R. (2018) A practical framework for implementing e-commerce in SMEs in developing countries: a case from Bangladesh. *Academic Journal of Science* 8(2): 275–290.

Voigt, P. & von dem Bussche, A. (2017) *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer. Available from: **https://doi.org/10.1007/978-3-319-57959-7** [Accessed 21 June 2025].

Maximum rating: -   Permalink   Reply

Powered by Moodle

Chat to us!