Initial Post

Initial Post

by Tahmeed Ali - Sunday, 15 June 2025, 9:07 PM

Having read *Doroiman and Sirghi (2024)* and other sources, here are my thoughts regarding the questions asked.

What do you consider as a fully digital enterprise?

An enterprise is *digital* if it applies digital technology in its business models or in some of its functions, such as for data management, communication, service delivery and customer engagement (Cognizant, 2025). Thusly, an enterprise is *fully digital* if digital technology is applied in *all sections of the business*. Generally, this may also mean there is no reliance on manual (i.e. non-digital) processes. Often, a fully digital enterprise may just be referred to as "digital", rather than "fully digital" (Consultancy, 2025).

Of note, Doroiman and Sirghi (2024) in particular describes four main digitalisation directions in describing the progression of EU member states: skills, infrastructure, transformation of businesses, and public services.

What are the cyber security challenges/concerns with a fully digital enterprise?

A fully digital enterprise inherently has more digital domains as a proportion of the business to consider - this means more areas of attack to take care of as a defensive security specialist (ENISA, 2023). Gartner (2022) reports in particular high risks involving cloud-based software, open-source code and the supply chain network.

Fully digital enterprises also need to manage redundancies carefully, since they may not by their nature rely on physical barriers to entry or offline redundancies such as paper trails; this heavily impacts the *availability* of the CIA triad, and attacks like DoS could completely paralyse the business (NIST, 2024).

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

Small and medium-sized enterprises, or SMEs, in the United Kingdom refer to businesses with fewer than 250 staff and a turnover of at most £44 million (or a balance sheet total of at most £38 million) (Gov, 2023). As such, a lack of resources for investing in decent IT support and in training for staff, who may lack the necessary information to handle cybersecurity issues, is a major challenge to any SME (ENISA, 2021). This is especially true of a bricks-and-mortar SME, for which the employee requirements would not have included the technical know-how as standard. This lack of training (and a lack of checking for the required knowledge) makes employees especially vulnerable to social engineering attacks - where threats are to do with human behaviour instead of technical misconfigurations - such as phishing, pretexting and baiting.

Some common frameworks, such as the NIST Cybersecurity Framework (NIST, 2024) and ISO/IEC 27001 (ISO, 2022), take these issues into consideration by emphasising risk-based, scalable controls, and keeping staff informed of basic technical hygiene - making them accessible to such organisations with limited cybersecurity expertise.

References

Cognizant (2025) *Digital business*. Available at: https://www.cognizant.com/us/en/glossary/digital-business

Consultancy (2025) *The five fundamentals of becoming a Digital Enterprise*. Available at: https://www.consultancy.eu/news/11542/the-five-fundamentals-of-becoming-a-digital-enterprise

Doroiman, M.M. and 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. Available at: http://doi.org/10.47535/1991ojbe194

Gartner (2023) *Gartner Identifies Top Security and Risk Management Trends for 2022*. Available at: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

Gov (2023) *Procurement Act 2023*. Available at: https://www.legislation.gov.uk/ukpga/2023/54/section/123

ISO (2022) *ISO/IEC 27001:2022 - Information security management systems*. Available at: https://www.iso.org/standard/27001

Permalink Reply

Re: Initial Post

by Lauren Pechey - Saturday, 21 June 2025, 1:31 PM

Hi Tahmed,

Thank you for your insights about the cybersecurity risks for both fully digital companies and SMEs making the digital leap.

Just to add, for fully digital businesses, using a “zero trust” approach—where nothing is automatically trusted and every access is checked—can really help stop attacks before they spread (Gartner, 2023). Also, having smart systems that spot threats quickly, like ransomware, is super important (Gartner, 2023).

For SMEs, I totally agree that training staff to spot phishing and scams is key. Frameworks like NIST or ISO 27001 can be great because they are flexible and do not require huge resources. Moreover, working with security experts outside the company can give smaller businesses extra support they might not have in-house.

What are your thoughts on these ideas?

Kind regards,

Lauren Pechey

References:

Gartner. (2023) Gartner Identifies Top Security and Risk Management Trends for 2022. Available from: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022. [Accessed 21 June 2025].

Maximum rating: -

Permalink Show parent Reply

◀ Initial Post

You are logged in as Lauren Pechey (Log out)

Policies

Powered by Moodle

Site Accessibility Statement
Privacy Policy