Task 'Initial Post Collaborative Security Implications of the Digital Economy'

Unit 1

'Initial Post'

What do you consider as a fully digital enterprise?

A fully digital enterprise automates all core business functions using digital technologies, from customer interaction and supply chain management to and internal operations, such that digital systems are essential rather than supplementary, today this may include cloud-based platforms, digital payment systems, CRM/ERP integration, e-commerce, big data analytics, and automation across processes.

As reflected by the Digital Economy and Society Index (DESI) digital intensity and technology adoption indicators. In a fully digital enterprise, real-time data supports strategic decision-making, with minimal reliance on paper-based or manual processes.

(Doroiman and Sîrghi, 2024).

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

While the author focuses on economic outcome aspects, some literature highlights the significant concerns that digitalization cybersecurity and data processing introduces.

Task ‘Initial Post Collaborative Security Implications of the Digital Economy’

Unit 1

The value of a fully digital enterprise depends on Integrity, Confidentiality, and Availability, with threats including ransomware, supply-chain attacks, phishing, and insider misuse. These risks are inherent and natural consequences of digital dependency, rather than factors explicitly analyzed within the DESI framework.

(Doroiman and Sîrghi, 2024; PwC, 2023)

Technologies such as cloud computing and electronic information systems are central to digital performance, but they also expand organizational attack surfaces, and without clear visibility, effective risk-based and security controls, negative events could disrupt operations, undermine trust and lead to regulatory concerns; for instance, regulations that require organizations to ensure resilience are therefore critical governance complements to digital adoption.

(George et al., 2024)

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

For bricks-and-mortar SMEs transitioning to digital models, these challenges are intensified by limited resources, skills gaps, and immature risk-management practices. SMEs may end up adopting digital tools without an effective security architecture will increase risk exposure to third-parties, cloud misconfiguration, identity theft and more. Digital adoption remains a challenge, insufficient attention to cybersecurity and governance can create operational, reputational, and social risks, including workforce

exclusion and skills inequality. Addressing these issues requires technological investment, training and external support.

In summary, the author examines how enterprise digitalization influences EU economic growth using DESI and Eurostat data, showing uneven growth effects and the central role of labor productivity. Extending their findings, ethical, social, and security considerations could emerge as critical contextual factors shaping the sustainability of digital transformation.

(Doroiman and Sîrghi 2024)

References

- 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.
- George, A.S., Baskar, T. and Srikaanth, P.B., (2024). *Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors*. Partners Universal International Innovation Journal, 2(1), pp.51-75. Available at: DOI: https://doi.org/10.5281/zenodo.10639463 [Accessed: 28 January 2026].
- Price Waterhouse Coopers (PwC) (2023) *Global Digital Trust Insights Survey 2023*. Available at: https://www.pwc.de/de/im-fokus/cyber-security-privacy/pwc-digital-trust-survey-2023.pdf [Accessed: 27 January 2026].