Fully Digital Enterprise & Cybersecurity

Founded in 1997 as a DVD rental service, Netflix has transformed into a global streaming giant with over 17.3 million subscribers in the UK alone (Statista, 2024). A fully digital enterprise integrates digital technologies across all operations, using automation, AI, cloud computing, and IoT to enhance efficiency and decision-making (Doroiman & Sîrghi, 2024). Netflix embodies this by running its IT infrastructure on Amazon Web Services (AWS), eliminating physical data centres and enabling global scalability (Netflix Tech Blog, 2016). AI-driven algorithms personalise content recommendations and optimise production choices (Gomez-Uribe & Hunt, 2015).

Cybersecurity Risks in a Digital Enterprise

- Data breaches are a major threat due to large amounts of stored customer and business data.
- Ransomware & AI-powered attacks: Attackers exploit vulnerabilities to lock systems and demand payment (Doroiman & Sîrghi, 2024).
- Misconfigurations and weak access controls can expose sensitive data.
- Reliance on third-party vendors increases risks, as flaws in a partner's system can affect interconnected platforms.
- Compliance with regulations like GDPR and NIS2 is complex but essential to avoid penalties and reputational damage.
- Attackers can manipulate algorithms or exploit automated processes for large-scale attacks.

Cybersecurity Challenges for SMEs Going Digital

SMEs face several cybersecurity challenges as they transition to digital operations. Many lack the necessary expertise which leaves them vulnerable to attacks (ENISA, no date). Outdated IT systems also pose a risk as older infrastructure may not withstand modern cyber threats. Phishing and social engineering attacks are common. The move to online transactions increases the risk of fraud and data breaches making secure payment processing and strong encryption essential. Employees working remotely from unsecured networks can expose sensitive data without proper safeguards. Limited budgets make it difficult for SMEs to invest in advanced cybersecurity tools which heightens their vulnerability (NCSC 2019).

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, Volume IX(2), pp. 36–46.

Enisa (no date) SMEs Cybersecurity, Enisa. Available at: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity (Accessed: February 8, 2025).

Gomez-Uribe, C.A. and Hunt, N. (2015) “The Netflix Recommender System: Algorithms, Business Value, and Innovation,” ACM Transactions on Management Information Systems, 6(4). Available at: https://dl.acm.org/doi/pdf/10.1145/2843948.

National Cyber Security Centre (2023) NCSC launches flagship new services to help millions of small organisations stay safe online, National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/news/ncsc-launches-new-services-help-small-organisations-online (Accessed: August 2, 2025).

Pektaş, O.İ. (2021) The Story of the Migration of Netflix’s IT Resources to Cloud, netflixtechblog. Available at: https://medium.com/@onurinanpektas/the-story-of-the-migration-of-netflixs-it-resources-to-cloud-3af95dff9aac (Accessed: February 8, 2025).

Statista (2024) Netflix Households in the UK, Statista. Available at: https://www.statista.com/statistics/529734/netflix-households-in-the-uk/ (Accessed: February 8, 2025).