Initial Post

◀ Initial Post

Display replies in nested form

Settings ⌄

Initial Post

by Ruben Marques - Wednesday, 11 June 2025, 4:50 PM

Hello everyone!

Here are my conclusions from my readings and questions.

What do you consider as a fully digital enterprise?

The shift to a digital economy offers immense benefits but introduces significant cybersecurity challenges that require robust strategies to protect digital assets and ensure operational resilience.

A fully digital enterprise is an organisation that integrates technologies such as cloud, AI and IoT across its operations. Doroiman and Sîrghi (2024) establish the macroeconomic importance of this, linking digital intensity to economic growth while internally, this requires a strategic interchangeability between business and IT capabilities to reshape the firm's value proposition and competitive advantage to get behind a culture of innovation and continuous learning that adds robust security into its core governance (Spremić & Šimunić, 2018).

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

Deep integration of digital domains expand the entire attack surface, creating significant cybersecurity challenges. Key risks that come to mind include complex supply chain vulnerabilities, where flaws in development pipelines can be exploited (Kim, 2021) and a bigger exposure to data breaches and ransomware, which continue to be financially devastating (IBM Security, 2023). Furthermore, the reliance on digital channels increases susceptibility to sophisticated insider threats and social engineering attacks, while navigating complex regulatory standards like GDPR remains a constant pressure (Spremić & Šimunić, 2018).

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

For traditional SMEs the path to secure implementations is very different, with the primary challenge being their limited resources for cybersecurity investment (ENISA, 2021). This also adds low employee cybersecurity awareness on top, which makes them highly susceptible to phishing attacks for example, a primary threat vector in today's scope and to manage these challenges a structured path is essential (Reinheimer, Zorzo & De Bona, 2022).

The NIST Cybersecurity Framework (NIST, 2024) provides this, allowing SMEs to adopt a phased approach by Identifying critical assets and risks, Protecting them with basic controls and training, implementing tools to Detect incidents, develop plans for Response and finally, ensure they can Recover business operations.

References

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. MIS Quarterly, 37(2), pp. 471–482.

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.

ENISA - European Union Agency for Cybersecurity. (2021). Cybersecurity for SMEs: Challenges and Recommendations. Available at: **https://www.enisa.europa.eu/publications/cybersecurity-for-smes**

IBM Security. (2023). Cost of a Data Breach Report 2023. Available at: **https://www.ibm.com/reports/data-breach**

Kim, M. (2021). A study on security vulnerabilities of CI/CD pipeline and its security enhancement. Journal of The Korea Institute of Information Security and Cryptology, 31(1), pp. 127–138.

NIST - National Institute of Standards and Technology. (2024). Cybersecurity Framework Version 2.0. Available at: **https://www.nist.gov/cyberframework**

Reinheimer, B., Zorzo, A., & De Bona, L. (2022). Cybersecurity for SMEs: A systematic review of challenges and recommendations. Journal of Information Security and Applications, 68, 103233.

Spremić, M., & Šimunić, I. (2018). Toward a holistic cyberculture: Integrating cybersecurity into business governance. Information & Management, 55(7), pp. 854–865.

Chat to us!

Permalink Reply

Re: Initial Post

by Beran Necat - Thursday, 12 June 2025, 8:46 PM

Hi Ruben,

Many thanks for your interesting post.

In addition, following the pandemic, cybersecurity concerns emerged from a far greater volume of online retail transactions. Many businesses rushed their development of applications and platforms in response to the COVID-19 pandemic (Geer, 2021; Linthicum, 2021). Developers were pressured to release applications and security patches to meet a timeline, as opposed to completing testing and vulnerability analysis (Security Compass, n.d.). This also led to a unique phenomenon where approximately 25% of zero-day patches produced in 2020 were the result of insufficient investigation; in other words, approximately one third of all zero-day patches failed to identify the root cause of the exploit (Stone, 2021). Because of this, attackers have been able to make minor tweaks to exploits to circumvent security patches (Security Compass, n.d.; Stone, 2021).

Like many of us, I witnessed this with many of the collaboration and virtual meeting software pushing out glitchy patches to keep up with demand!

Regards, Beran

References

Geer, D. (2021). Rushed digital transformation is creating security risks. [online] Hewlett Packard Enterprise. Available at: https://www.hpe.com/us/en/insights/articles/rushed-digital-transformation-is-creating-security-risks-2111.html. [Accessed 12 June 2024].

Linthicum, D. (2021). The pandemic-driven rush to cloud is compromising security. [online] InfoWorld. Available at: https://www.infoworld.com/article/3612245/the-pandemic-driven-rush-to-cloud-is-compromising-security.html. [Accessed 12 June 2025].

Security Compass. (n.d.). Google: Insufficient and rushed patching leads to more zero-day exploits. [online] Available at: https://www.securitycompass.com/in-the-news/google-insufficient-and-rushed-patching-leads-to-more-zero-day-exploits/ [Accessed 12 June 2025].

Permalink Show parent Reply

Peer Response

by Ruben Marques - Friday, 13 June 2025, 12:44 PM

Hello Professor,

That's a great real-world observation. The rushed shift during the pandemic left a lot of security gaps, and the Colonial Pipeline attack in 2021 is a perfect example of what can go wrong if initial security measures are ignored.

The Colonial Pipeline runs a massive fuel pipeline that supplies a large part of the eastern United States. In May 2021, a ransomware attack forced them to shut down the entire pipeline, leading to widespread fuel shortages and panic buying (Bellamkonda, 2024).
The most shocking part was how the hackers got in. It wasn't through some highly complex flaw. They gained access using a single stolen password for an old, unused remote work account. Crucially, that single account was not protected by Multi-Factor Authentication (MFA), which would have potentially stopped the attack (Bellamkonda, 2024).

This ties directly into your point about the pandemic rush. In the chaos of setting up widespread remote work, organizations often prioritized operational speed over security, leading to exactly these kinds of oversights (Lallie et al., 2021). It's easy to see how an old account could be overlooked or how enforcing a basic security policy like MFA might have been put on the back burner in favor of just getting things working.

It’s a powerful lesson. If a massive, critical infrastructure company can be brought down by such a basic oversight, it really highlights how vulnerable a small business with far fewer resources is. It proves that foundational security measures such as the "Protect" functions outlined in frameworks like NIST (NIST, 2024) aren't just a formality. They are often the one thing standing between normal operations and a complete disaster.

References

Bellamkonda, S. (2024). Ransomware Attacks On Critical Infrastructure: A Study Of The Colonial Pipeline Incident. INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND INFORMATION TECHNOLOGY, 7, pp. 1423-1433.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Belle, A. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

NIST - National Institute of Standards and Technology. (2024). Cybersecurity Framework Version 2.0. Available at: https://www.nist.gov/cyberframework

Permalink Show par

Re: Peer Response

by Lauren Pechey - Saturday, 19 July 2025, 6:57 PM

Hi Ruben,

Thank you for your contribution! Your post does a great job highlighting both the promise and the challenges of becoming a fully digital enterprise. I appreciate how you link the macroeconomic benefits with the internal need for firms to align IT and business capabilities, which shows you understand that digitalisation is more than just technology adoption. Your points on the increased attack surface, supply chain vulnerabilities, and insider threats are realistic and well supported by current sources.

I especially liked that you included the NIST Framework as a practical step for SMEs, which makes your response actionable, not just theoretical. One suggestion would be to add a quick example of how AI, IoT, or cloud are used in daily operations, just to ground your definition a bit more. Also, for SMEs, mentioning a low-cost security practice like multi-factor authentication or regular staff training could make your point even stronger. Overall, your response is clear, well-researched and directly addresses the main questions — excellent work.

Best of luck,

Lauren Pechey

Maximum rating: -

Permalink **Show parent** **Edit** **Delete** **Reply**

◀ **Initial Post**