SUMMARY POST

From Vulnerability to Resilience: Integrating Industry 5.0 Principles into Cybersecurity for Healthcare and Beyond

In my initial discussion, I examined the 2017 NHS WannaCry ransomware attack as a case study in Industry 4.0's double-edged nature. While AI, IoT, and digital systems have transformed healthcare delivery, the attack exposed dangerous dependencies on outdated, unpatched infrastructure. I argued for Industry 5.0's human-centric, resilient model, where technology augments rather than undermines professionals. Peer feedback expanded this view into actionable strategies.

One peer emphasised regular patching with clear accountability, network segmentation, and ongoing staff training, alongside cyber drills to improve real-time response (Smart, 2018; National Cyber Security Centre, 2023). Clarke and Martin (2023) likewise highlight the need for comprehensive training on cybersecurity best practices, strong password management, and phishing detection. In the NHS, such training should engage clinicians, administrators, and IT professionals to ensure relevance and proper resource allocation. Simulations can further help staff identify latent threats in both training and practice.

Another peer stressed live device inventories, rapid emergency patching, and embedding security into system design aligned with the UK's 2030 cyber resilience plan (Department of Health and Social Care, 2023). Fostering clear communication channels between IT teams and end users is also vital for collaborative security awareness (Clarke and Martin, 2023). Responding to others' incidents broadened my perspective. In discussing remote workforce monitoring, I advocated for user-centred design, GDPR compliance, and wellbeing-focused boundaries (Anshari et al., 2021; O'Connell, 2024).

In a biotech case, I proposed proactive training, Zero-Trust security, and cyberbiosecurity measures such as encryption and SQL/XSS prevention (Kosaraju, 2025; Laith et al., 2025). These experiences reinforced that cyber resilience depends on both robust technical safeguards and ethical, human-centred design. As Merchán-Cruz et al. (2025) propose in their "Trust by Design" framework, embedding ethics, privacy, and accountability throughout the system lifecycle embodies the core principles of Industry 5.0. In doing so, intelligent systems can be designed to reliably augment rather than undermine the professionals and communities they serve, ensuring innovation strengthens both technological resilience and human trust.

REFERENCES

Anshari, A., Hirtranusi, S.A., Sensuse, D.I. and Suryono, R.R. (2021) 'Designing an Attendance System Model for Work from Home (WFH) Employees Based on User-Centered',International Conference on Computer Science, Information Technology, and Electrical Engineering pp. 125-132.

Clarke, M. and Martin, K. (2024) 'Managing Cybersecurity Risk in Healthcare Settings', Healthcare Management Forum 37(1), pp.17-20.

Department of Health and Social Care, 2023. A cyber resilience strategy for health and social care: 2023 to 2030. London: Department of Health and Social Care.

Kosaraju, P. (2025) ‘Safeguarding OT Networks in Biotech Manufacturing Plants’, Journal of Computer Science and Technology Studies 7(3), pp.972-981.

Laith, A.E., Jaouni, H. and Mihyar, A. (2025) ‘Addressing Cyberbiosecurity Challenges in the Modern Era of Biotechnology and Artificial Intelligence: Cyberbiosecurity in the Age of Biotechnology and AI. Global Biosecurity.

Merchán-Cruz, E.A., Gabelaia, I., Savrasovs, M., Hansen, M.F., Soe, S., Rodriguez-Cañizo, R.G. and Aragón-Camarasa, G. (2025) ‘Trust by Design: An Ethical Framework for Collaborative Intelligence Systems in Industry 5.0’ Electronics14(10), p.1952.

National Cyber Security Centre (2023) Cyber security for healthcare organisations. London: NCSC.

O'Connell, E. (2024) Does Employee Monitoring Infringe on Workers’ Right to Privacy, While Working from Home? PHD thesis.

National College of Ireland. Available at: https://norma.ncirl.ie/7889/1/elizabethoconnell.pdf (Accessed: 14th August 2025).

William, S. (2018) Lessons Learned Review of the WannaCry Ransomware Cyber Attack. Independent Report. London: Department of Health and Social Care.