Industry 4.0 Discussion – Initial Post

Industry 4.0 is described by Kovaite and Stankeviciene (2019) as the latest industrial revolution, driven by technologies like the Internet of Things (IoT), big data, cloud computing, robotics and Artificial Intelligence (AI).

Particularly notable is how it redefines interactions between human and machines, moving towards a decentralized model of communication. This has various impacts on the workforce, particularly in how digital knowledge will be demanded, which will lead to changes in education and training (Sima *et al*., 2020).

Automated warehouses that use robots to ferry products and IoT sensors on conveyor belts are an example of these technological drivers in action, as is the use of AI and big data in supply chains to analyse trends.

Industry 4.0 does bring additional risks, and these have been exploited. In 2014 a German steel mill's network was compromised via a spear phishing email. Once inside the network the attacker was able to disrupt numerous systems, including the system that controlled the blast doors. In 2019 Norsk Hydro Aluminium's systems were affected by ransomware, and company access disabled (Oueslati *et al*., 2019).

Singh and Kumar (2025) agree with Kovaite and Stankeviciene that advancements brought by Industry 4.0 technological drivers add security vulnerabilities, and that mitigating these new areas of attack is crucial to preserving the reliability and usability of industrial processes. Somewhat worryingly, and despite being published 6 years later, they echo the belief that there are significant research gaps on many of the new attack surfaces.

References

Kovaite, K. and Stankeviciene, J. (2019) 'Risks of Digitalisation of Business Models', Proceedings of the 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering (CIBMEE-2019), 9-10 May, Vilnius, Lithuania. Vilnius: VGTU Press. Available at: https://doi.org/10.3846/cibmee.2019.039

Oueslati *et al*. (2019) 'Comparative Study of the Common Cyber-Physical Attacks in Industry 4.0,' *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, Tunis, Tunisia. Pp. 1-7. Available at: https://doi.org/10.1109/IINTEC48298.2019.9112097

Sima *et al*. (2020) 'Influences of the Industry 4.0 Revolution on the Human Capital Development and Consumer Behaviour: A Systematic Review', *Sustainability*, 12(10), 4035. Available at: https://doi.org/10.3390/su12104035

Singh, B. and Kumar, B. (2025) 'Navigating Cybersecurity Risks in Industry 4.0: Challenges, Threats and Defense Strategies', Journal of Information Systems Engineering and Management (JISEM), 10(19s). Available at: https://doi.org/10.52783/jisem.v10i19s.3018