COLLABORATIVE DISCUSSION 1: THE FOURTH INDUSTRIAL REVOLUTION

(SUMMARY POST)

Murthy Kanuri
Machine Learning
University of Essex

In the initial post, I explored the views of Klaus Schwab (2016) regarding the Fourth Industrial Revolution. This section weighed the potential disruptions that advanced technologies such as artificial intelligence, machine learning, robotics, and the Internet of Things have on society, business, and government. To this end, Schwab asserts that there is fast-paced progress in such technologies, which, on the contrary, poses both challenges and opportunities. I also highlighted an essential feature of this new era, potential threats, by discussing the ransomware attack, commonly called WannaCry, that targeted the National Health Service in 2017. The attack resulted in cancellations of massive appointments and significant delays of the emergency services, with an estimated loss of around £92 million (Campbell, 2017; Hern, 2017; National Audit Office, 2018). It also created a lack of faith in the safety of such systems and stressed that better protection against hacking would be needed (Ikezuruora, 2024).

In his feedback, Ben mentioned the implications and access to the individuals' personally identifiable data due to the effect. Ben mentioned the NHS'e efforts to isolate the network to avoid the ransom payment. However, there is concern about patient data being accessible to the attackers; in addition, Ben underscored the importance of using methods such as encryption to restrict the exposure of confidential information during such onslaughts in the NHS (NHS, 2023). He also put forward a pertinent query on what institutions should do to lessen the threats posed by being interlinked with devices (Ikezuruora, 2024).

Martyna explained the need for isolated backups and network segmentation as essential security measures on these two bases. She illustrated how the WannaCry spread demonstrated the need to adhere to patch management and frequent updates (Mohurle & Patil, 2018). She also mentioned that the breach would have had fewer consequences with network segmentation, and thus, the NHS could have navigated through the chaos faster. Her points proved the need for layered and active defences in an increasingly interconnected world (Kharraz et al., 2015; Basta et al., 2021).

Both contributions also extended the debate by including specific actions that could be taken to combat threats to sensitive data and business continuity—for example, encryption, isolated backups, and network segmentation. The feedback suggests that a comprehensive approach to cybersecurity is needed to face the challenges of the Fourth Industrial Revolution.

References

- Basta, N., Ikram, M., Kaafar, M.A., & Walker, A. (2021). *Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework.* Available at: https://arxiv.org/pdf/2111.10967 (Accessed: 5 November 2024).
- Campbell, D. (2017). *NHS seeks to learn lessons after cyber-attack chaos*. The Guardian, 15 May. Available at: https://www.theguardian.com (Accessed: 26 October 2024).
- Hern, A. (2017). *NHS cyber-attack: everything you need to know about "WannaCry" ransomware*. The Guardian, 12 May. Available at: https://www.theguardian.com (Accessed: 26 October 2024).

- Ikezuruora, C. (2024). *The Hidden Costs: Understanding How Data Breaches Affect Customer Trust and Brand Reputation*. Available at: https://www.privacyend.com/data-breaches-affect-consumer-trust-brand-reputation/ (Accessed: 28 October 2024).
- Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.* In *Detection of Intrusions and Malware, and Vulnerability Assessment*, 9148, pp. 3-24. Available at: https://doi.org/10.1007/978-3-319-20550-2_1 (Accessed: 5 November 2024).
- Mohurle, S., & Patil, M. (2018). *A Brief Study of WannaCry Threat: Ransomware Attack 2017.* SBGS Media. Available at: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf (Accessed: 5 November 2024).
- National Audit Office (2018). *Investigation: WannaCry cyber attack and the NHS.* National Audit Office Report, 27 March. Available at: https://www.nao.org.uk (Accessed: 5 November 2024).
- NHS (2023). *NHS England business continuity management toolkit case study: WannaCry attack.* Available at: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ (Accessed: 5 November 2024).
- Schwab, K. (2016). *The Fourth Industrial Revolution: what it means and how to respond.* World Economic Forum. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (Accessed: 5 November 2024).