Re: Peer Response

by Mariam Ibrahim Ismail Hasan Almarzooqi - Sunday, 19 October 2025, 2:41 PM

Hi,

Thank you for your thoughtful post on the transition from Industry 4.0 to Industry 5.0 in manufacturing. Your example of the WannaCry ransomware attack on Nissan is a strong reminder of the vulnerabilities that come with increased digital integration. As you rightly noted, while Industry 4.0 brought incredible efficiency through IoT and automation, it also introduced new cybersecurity challenges (Farion-Melnyk et al., 2021; Reinhold, 2024).

I appreciate your point about the reputational damage Nissan suffered. Nwankpa and Schooley (2025) emphasize that repeat cybersecurity incidents often occur because of inadequate long-term risk planning and the underestimation of evolving cyber threats. The shift toward Industry 5.0 is essential in this context, not just for improved technological systems, but for restoring human oversight, adaptability, and ethical responsibility in crisis management (Vatsyayan et al., 2022).

Adding human-centric resilience—such as training employees in cyber hygiene, developing hybrid human-AI monitoring systems, and enhancing rapid response protocols could be vital in preventing future attacks (Aljaidi et al., 2022). As we move forward, the combination of automation and ethical, sustainable human input will be key to ensuring both security and trust in manufacturing systems.

Great analysis this is a powerful example of why cyber resilience must evolve alongside technological progress.

Reference:

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y. A. (2022, November). *NHS WannaCry ransomware attack: Technical explanation of the vulnerability, exploitation, and countermeasures.* In 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI) (pp. 1–6). IEEE.

Farion-Melnyk, A., Rozheliuk, V., Slipchenko, T., Banakh, S., Farion, M., & Bilan, O. (2021, September). *Ransomware attacks: Risks, protection, and prevention measures.* In 2021 11th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 473–478). IEEE.

Nwankpa, J., & Schooley, J. (2025). *Understanding the antecedents of repeat data breach incidents for firms.*

Reinhold, T. (2024). WannaCry: About the tragedy of the commons? In *Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons* (pp. 185–196). Springer Fachmedien Wiesbaden.

Vatsyayan, V., Chakraborty, A., Rajarajan, G., & Fernandez, A. L. (2022). *A detailed investigation of popular attacks on cyber-physical systems.* In Cyber Security Applications for Industry 4.0 (pp. 1–42). Chapman and Hall/CRC.

Maximum rating: -

Permalink | Show parent | Edit | Delete | Reply