Peer Response 1

In his post, Linga effectively explains the Fourth Industrial Revolution, acknowledging that while it opens new opportunities, it also presents significant challenges. He discusses the WannaCry attack on the National Health Service (NHS)—a case I wasn't previously familiar with—which made for an enlightening read. Linga clearly outlines the patient implications, as well as the economic and reputational costs incurred from this incident.

As Ben points out, the attackers demanded a ransom; although it wasn't paid and the data was eventually recovered, the process was immensely challenging (Mohurle & Patil, 2018). This underscores the importance of implementing isolated backups. Such backups would not only prevent the NHS from having to pay a ransom in future incidents but would also expedite system restoration, minimizing service disruptions and reducing economic impact (Kharraz et al., 2015).

One particularly concerning aspect of this incident was the rapid spread of WannaCry's malware across networks and devices (National Audit Office, 2017). This highlights the critical role of network segmentation, patch management, and regular updates. Network segmentation is crucial in the event of a security breach, as it contains the attack within a limited section of the network, reducing the overall impact on the institution. Linga notes that one result of the attack was widespread appointment cancellations. With effective network segmentation, the attack's reach would be more contained. While some appointments might still be affected, the disruption would be significantly less, allowing for a quicker recovery and fewer delays (Basta et al., 2021).

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 Nov. 2024)

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. & Kirda, E., (2015). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*. 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 Nov. 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 Nov. 2024).

National Audit Office, (2017). *Investigation: WannaCry cyber attack and the NHS*. Available at: **https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/** (Accessed 5 Nov. 2024)

Peer Response 2

In his post, Guilherme highlights the transformative potential of the technological revolution in healthcare, emphasizing benefits such as improved scheduling, optimized resource allocation, and faster decision-making — all critical for the timely implementation of treatments that increase patient recovery chances (Seymour et al., 2017). However, as he correctly notes, deploying these technological solutions carries inherent risks, particularly related to data breaches and cyberattacks. Public healthcare organizations are especially vulnerable, given the extensive amounts of sensitive data they manage (Duguin, 2021). The recent Synnovis incident, which Guilherme references, exemplifies this vulnerability. In that case, patient care was disrupted as certain essential tests could not be performed due to a cyberattack.

Such incidents, while impactful, are preventable, though ensuring adequate security demands multiple proactive actions. Cyber attackers frequently exploit software vulnerabilities, making it crucial for healthcare systems to prioritize regular security measures. Software should undergo routine testing to identify existing vulnerabilities, and security patches must be promptly applied and verified to minimize risk (Al Qartah, Alenezi & Al-Anzi, 2021). This proactive approach could prevent incidents like Synnovis.

Employee awareness and training are also essential to safeguarding sensitive data. Phishing attacks, despite advancements in detection systems, still pose a significant threat. Healthcare professionals, often trained primarily on specific software for clinical use, may lack awareness of cybersecurity practices. This gap is concerning, especially since studies indicate that 65% of healthcare employees targeted by phishing clicked

on at least two suspicious emails, exposing sensitive data to significant risks (Verma, Kumar & Kishore, 2020).

These are just two examples of the preventive measures that could have mitigated the Synnovis incident. I encourage Guilherme to delve deeper into other protective strategies in his ongoing research, as a comprehensive approach is vital to securing healthcare systems in an era of digital transformation.

References:

Al Qartah, R., Alenezi, M. & Al-Anzi, F.S., (2021). *A framework to mitigate cybersecurity risks in healthcare systems*. *Information & Management, 59(3),* p.103430. Available at: https://doi.org/10.1016/j.im.2021.103430 (Accessed 4 Nov. 2024)

Duguin, S., (2021). *If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition. World Economic Forum*. Available at: https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/ (Accessed 4 Nov. 2024).

Seymour, C.W., Gesten, F., Prescott, H.C., Friedrich, M.E., Iwashyna, T.J., Phillips, G.S., Lemeshow, S., Osborn, T., Terry, K.M. & Levy, M.M., (2017). *Time to treatment and mortality during mandated emergency care for sepsis*. New England Journal of Medicine, 376(23), pp.2235-2244. Available at: https://doi.org/10.1056/NEJMoa1703058 (Accessed 4 Nov. 2024)

Verma, M., Kumar, D. & Kishore, K., (2020). *Cybersecurity in health care: A narrative review. Indian Journal of Public Health, 64(2),* pp.149–155. Available at: https://doi.org/10.4103/ijph.IJPH_410_19 (Accessed 4 Nov. 2024).