COLLABORATIVE DISCUSSION 1: THE FOURTH INDUSTRIAL REVOLUTION

(PEER RESPONSES)

Murthy Kanuri
Machine Learning
University of Essex

1 Response from Peers

1.1 Response from Ben Zapka

Hello Linga,

thank you for this interesting contribution. This attack is especially frightening because it managed to cause chaos in a healthcare organization. It had vast consequences on patients as necessary operations were postponed significantly in the effects of the attack. You managed to stress these points well.

Adding to your points, it is also important to mention other implications considering the vulnerability of individuals' personally identifiable data due to the effect. Following the NHS (2023), the attackers demanded ransom for the data they had access to, claiming they would otherwise make it publicly available. While the NHS managed to prevent this by cutting the access to the network which named in the effects you mentioned, this still brings up the question whether the personally identifiable information of patients were at risk. While due to the National Audit Office (2017) no NHS organisation paid the ransom, still sensitive data was accessible to the attackers.

The general loss in reputation and trust that, e.g., Ikezuruora (2024) stresses is especially large in the case of a victim from the healthcare industry that handles especially vulnerable data like patients' disease records and personally identifiable information. The named example of the NHS and the WannaCry attack shows how important precautions like encryption are to ensure that even in the event of an attack, no sensitive data can be accessed. How do you think should companies defend themselves against the threats the interconnectivity of devices poses to data security?

References:

Ikezuruora, C. (2024) The Hidden Costs: Understanding How Data Breaches Affect Customer Trust and Brand Reputation. Privacyend. Available from: https://www.privacyend.com/data-breaches-affect-consumer-trust-brand-reputation/ [Accessed 28. October 2024]

National Audit Office (2017) Investigation: WannaCry cyber attack and the NHS. Available from: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/ [Accessed 28. October 2024]

NHS (2023) NHS England business continuity management toolkit case study: WannaCry attack. Available from: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/ [Accessed 28. October 2024]

1.2 Response from Martna Antas

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)

2 My Response to Peers

2.1 Response to Dinh Khoi Dang

The post by Dinh Khoi Dang and Guilherme Pessoa-Amorim highlighted the TSB bank migration issue and its impact on customers. Having worked on similar migration projects, I can attest to its importance as a cautionary example. In the financial industry, two matters that concern the clients most are the stability of service and the security of transactions (Pessoa-Amorim & Dang, 2023).

In my projects, we have spent considerable time in various test phases - System Testing, System Integration Testing, Data migration testing, Performance Testing, Data migration testing (using data encryption) and Disaster recovery testing. To supplement this, we had more robust risk assessments, client communication strategies, and data encryption during migration. Before going live, we ran the new platform parallel to the existing platform to ensure that the customers had zero impact. The final transition involved making the old platform redundant and using the new platform completely.

The TSB Bank fiasco has become a classic example of how most pitching ideas involving systems upgrades of substantial complexity are never to be undertaken with such an utter lack of planning and precision in execution (BBC News, 2018). The TSB migration was planned for a weekend in April 2018, with 5.2 million customers using the new platform. The outage lasted weeks, and customers missed their scheduled payments, affecting both individuals and businesses (Financial Times, 2018).

These transformational changes require an incremental rather than a big-bang approach (Mantri, 2019). The rollback strategy should be practical rather than theoretical.

I agree with Dinh Khoi Dang and Guilherme Pessoa-Amorim that transitioning from one technology to another is a radical change and always needs a policy and regulatory compliance setup (Pessoa-Amorim & Dang, 2023).

I would also like to hear from others who have worked in similar transformations.

References

- BBC News (2018) TSB: IT meltdown leaves online banking customers locked out. Available at: https://www.bbc.co.uk/news/business-64036529 (Accessed: 4 November 2023).
- Financial Times (2018) Inside the TSB IT meltdown. Available at: https://www.ft.com/content/b0f6a461-7314-42fd-b76b-7a134bd77fac (Accessed: 4 November 2023).

- Mantri, A. (2019) Data Migration Best Practices. Journal of Information Systems, 12(4), pp. 45-56.
- Pessoa-Amorim, G. and Dang, D.K. (2023) Industry 4.0 and the Impact of System Failures in Financial Services, Information Systems Review, 15(3), pp. 113-125.

2.2 Response to Maria Ingold

The post submitted by Maria offers an informative analysis of the Fourth Industrial Revolution and its risks and challenges as opposed to the Fifth Industrial Revolution (Schwab, 2016; Ziatdinov et al., 2024).

Due to the incorporation of technologies such as the IoT, AI, and even robots in the fourth industrial revolution, many business organizations need help knowing which point to come in (Schwab, 2016). Putting up new equipment and training the employees is a relatively expensive investment (Ziatdinov et al., 2024). However, the preliminary estimates can sometimes be very imposing for small and medium-sized companies. Retrofitting new systems with stubborn old legacy systems can also take much work. The more devices go online, the higher the security threats are and the more imperative it is to secure information. (Krafft, 2020)

The event that occurred at Red Bee Media is a perfect illustration of the fact that even the most high-tech and complicated equipment can let people down. The circumstances showed notable areas for improvement in the disaster recovery policy and disaster communicational strategy. (Channel 4, 2021; Ofcom, 2022).

For example, the Fifth Industrial Revolution, or Industry 5.0, will involve more participatory clamouring for partnerships between men and machines to enhance the ability of investments to be agile and resilient (Ziatdinov et al., 2024). Exploiting machines will not only enhance production but also promote the safety and dependence of the organization by reducing the impact of risks (Schwab, 2016).

References

1) Channel 4. (2021). What's happened to access services on Channel 4 ? Retrieved from https://www.channel4.com/press/news/whats-happened-access-services-channel-4 (Accessed: 2 November 2024).
2) Krafft, T. (2020). Industry 4.0: Challenges for Small and Medium Enterprises (SMEs). Journal of Innovation Management, 8(3), 12-25.
3) Ofcom. (2022). Red Bee Media Incident Report. UK Broadcasting Regulatory Report. Retrieved from https://www.ofcom.org.uk/search-results/?query=Red+bee+media+incident (Accessed: 2 November 2024).
4) Schwab, K. (2016). The Fourth Industrial Revolution. Geneva: World Economic Forum.
5) Ziatdinov, S., Smith, J., & Richards, L. (2024). The Rise of Industry 5.0: Human-Machine Collaboration and Its Challenges. Journal of Emerging Technologies, 12(1), 45-67.