Peer Response

by Abdulrahman Alhashmi - Saturday, 9 August 2025, 8:41 PM

Your discussion of the NotPetya incident at Maersk demonstrates how disruptive cyberattacks can be when critical energy-related infrastructure is targeted. Avoiding such large-scale impacts requires a mix of technical safeguards, organisational readiness, and coordinated industry-wide strategies. One important step is separating operational control networks from corporate IT systems. This isolation limits the chance of a breach spreading across both domains (Cherdantseva et al., 2016). For a company like Maersk, keeping logistics and core operational platforms apart could have significantly reduced the damage.

Regular security audits and timely system updates are also crucial. Many serious incidents exploit weaknesses that are already known but remain unpatched due to operational delays (Abomhara and Køien, 2015). Enforcing strict update schedules and testing procedures can close these gaps.
Staff training on digital security threats is another essential measure. Since deceptive emails remain a common entry point for ransomware, targeted awareness sessions can help reduce the likelihood of an initial compromise (Tao et al., 2022).

Lastly, well-practised crisis response plans should be in place. Running scenario-based drills with all key personnel can reveal flaws in recovery strategies and allow for faster restoration of services in an actual emergency.

By combining advanced technical controls with a proactive, well-informed workforce, the sector can be better prepared to prevent or limit the scale of disruptions similar to the Maersk case.

References

Abomhara, M. and Køien, G.M., 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), pp.65-88.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, pp.1-27.

Tao, J., Wang, Y., Zhang, M., Luo, X. and Xu, Z., 2022. An empirical study on employees' susceptibility to phishing emails. Information & Management, 59(8), p.103667.

Peer Response

by Abdulrahman Alhashmi - Saturday, 9 August 2025, 10:27 PM

The WannaCry cyberattack was a significant moment. It showed how much healthcare relies on technology and how quickly time can slip away when systems fail. To prevent this from happening again, it's not just about fixing technical issues; it involves shifting habits and priorities across the board.

Let's start with the basics: updates. In 2017, many NHS computers were still running outdated versions of Windows, leaving them vulnerable to attacks. A stricter patch approval system and someone taking charge of non-patching could have greatly reduced the damage (Department of Health and Social Care, 2018).

Next is the human element: We've all accidentally clicked on something suspicious at some point; expecting staff to inherently know better isn't realistic. Regular short training sessions or reminders during shifts could help keep these risks fresh in employees' minds (NHS Digital, 2022).
What about effective network design? If key systems are isolated from the rest, an attack on one area doesn't need to affect everything else (National Cyber Security Centre, 2023).
Lastly, plans only work if they're practiced. Running a cyberattack drill might seem strange initially but could save crucial hours during an actual crisis.

References

Department of Health and Social Care (2018) Lessons learned review of the WannaCry ransomware cyber attack. London: DHSC.

National Cyber Security Centre (2023) Cyber security for healthcare organisations. London: NCSC.
NHS Digital (2022) Cyber security in the NHS: Best practice guide. Leeds: NHS Digital.

Peer Response

by Abdulrahman Alhashmi **- Sunday, 10 August 2025, 12:50 PM**

The case of the Evotec cyber-attack you described highlights how quickly digital reliance in biotechnology can turn into a major weakness. Thinking about what might have reduced the scale of the incident, a few practical measures stand out.

One would be adopting a zero-trust security model. In this setup, every attempt to access a system—whether internal or external—requires verification. This approach makes it much harder for attackers to move freely once they are inside the network (Rose et al., 2020).

Another safeguard is network segmentation. Keeping research data on an isolated network, separate from corporate or administrative systems, can limit the reach of an attack. This method has been effective in containing breaches within other pharmaceutical and biotech environments (Pinto, 2022). Regular incident response drills could also have helped. Running scenarios that involve both IT specialists and senior management builds familiarity with roles and speeds up decision-making when a real attack occurs (Parker, 2023).

Lastly, having immutable, secure backups stored offsite or in the cloud can make system restoration much faster. For a research-focused company with high-value contracts, this can mean the difference between meeting deadlines and losing clients.

What stands out here is that in an Industry 4.0 setting, resilience relies on more than advanced tools—it also depends on foresight, planning, and active human involvement. Industry 5.0's human-centred philosophy offers a stronger foundation for handling such risks.

References

Parker, L. (2023) 'Cybersecurity preparedness in pharmaceutical research organisations', Journal of Information Security Practice and Research, 15(2), pp. 45–58.

Pinto, R. (2022) 'Network segmentation strategies for critical infrastructure protection', International Journal of Cybersecurity, 8(3), pp. 122–135.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. Gaithersburg: National Institute of Standards and Technology.