Ashurst

Cyber in Rail
Roundtable discussion

22 April 2025

On 18 March 2025, Ashurst hosted a select roundtable discussion on Cyber in Rail (including representatives from Amey, Hitachi Rail, Keolis-MHI, a leading rail freight operator and a leading rail investor and developer) from which the following key themes emerged.

A changing threat landscape

Cyber security risks are made more challenging by the increasing complexity of the threat landscape. The roundtable discussion centred around agreement that the future of cyber threats to the rail industry is perhaps more likely to come in the form of large-scale *disruption* incidents, rather than data theft. Threat actors seem to be shifting their focus to exploit the vulnerabilities at the interface between IT to OT systems, allowing for more significant, public facing disruption.

With this particular kind of threat in mind some attendees reported increased concern in maintaining IT and OT systems separation, noting that OT often relies on older and more vulnerable systems. A key question for threat management is how far away is the industry from experiencing a significant incident that impacts an OT system, resulting in a sustained period of suspension and a long period of disruption, and how this level of threat can best be managed.

The rapid growth of AI capabilities adds complexity to the threat landscape, accelerating a threat actor's ability to infiltrate IT systems by sheer volume of attacks, as well as the potential to outpace the technical capabilities of companies and their boards.

Regulation

Attendees agreed that industry players may in fact welcome further regulation of the rail sector, if such regulation can help companies to prepare for and focus resources towards *cyber readiness*. This might help to unlock budget/spending to prepare for and mitigate cyber security threats.

Regulation presented as 'guidance' has long been a challenge for the industry, leaving companies in charge of both interpreting rules and regulations, as well as operationalising these principles. This 'principles based' approach to regulation has been a challenge to the rail industry, with companies often left to determine their own risk factors and implement guidance accordingly. Attendees hope that the UK's upcoming Cyber Security and Resilience Bill will make it clear which guidance documents should be prioritised/followed.

Attendees discussed the approach and possible impact of the UK's Cyber Security and Resilience Bill on the rail industry. Initial discussion suggested that the bill might place obligations on suppliers and subcontractors further down supply chains. This suggested that the UK government was beginning not only to acknowledge the significant threat of cyber attacks on Critical National

Infrastructure (including the rail industry), but also the likelihood that risks can arise from sub-suppliers even where a 'customer's' system is otherwise relatively secure. However, from a policy statement (issued on 1 April after the roundtable discussion) it now appears that the focus will be on the importance of simple and clear reporting requirements, with supply chain risk likely to be relegated to secondary legislation. The policy statement also confirms the Bill will broadly follow Europe's approach in the European Network and Information Security Directive 2 (NIS2) which means it will reach to rail infrastructure.

Discussion also touched on how public procurement processes may develop to encompass a company's 'cyber readiness'. Some attendees expect more oversight in procurement and bidding processes as to proof of robust cyber security controls, rather than simply relying on a company to assess its own risk and operationalise mitigations.

Communication with company boards

Attendees agreed that, although rail counts as critical infrastructure, the industry suffers from a lack of coverage in publicly available threat intelligence and reporting. This means it is often difficult for companies to provide accurate threat landscape reports to send to company boards. Attendees discussed that it is often manageable to evaluate the potential impact of a cyber attack, but visibility and a true understanding of the threat landscape, potential actors and their capabilities is difficult to express to boards. Approaches to effective communication with boards around cyber risk can include, as discussed, (i) extrapolating from public intelligence in other sectors, as there is often cross-industry applicability and (ii) beginning with a base level risk assessment which is then frequently updated as a better understanding of threat actors and their capabilities develops.

AI

Attendees explored the evolving role of AI in the cyber threat landscape. AI is increasingly being leveraged by threat actors to enhance the volume and impact of cyber-attacks, and whilst AI is not yet capable of generating significant attacks independently, its role in facilitating more believable and harder-to-detect phishing and malware attacks cannot be disputed. This democratisation of cyber-attack capabilities means that even less experienced actors can now launch effective attacks. The market is experiencing an increase in deep fake fraud and other AI-driven cyber threats, highlighting the need for robust cyber readiness strategies.

Attendees discussed the increased use of AI within their own organisations and how the risk landscape is continuously evolving. Data poisoning, where malicious actors deliberately alter training sets for AI systems, is one of the leading threats from increased use in AI systems. This can lead to compromised AI models that favour the outcomes desired by attackers. Further, continually learning AI systems can be manipulated over time to develop biases that benefit threat actors, posing a significant risk to businesses relying on AI for cybersecurity. Businesses must proactively address these emerging threats by incorporating AI risks and controls into their cyber readiness strategies and ensuring board members are engaged in cybersecurity discussions.

Conclusion

This is the first in what we hope will be a series of small roundtable discussions on Cyber in Rail alongside our focus on AI in Rail. Throughout 2025, we hope to cover the topics below and would appreciate your views on what would be of most relevance:

- **What good cyber readiness looks like and how to assess readiness within the rail industry;**
- **AI governance, risk management and literacy; and**
- **Building risk into contracts.**

We are also keen to discuss your specific AI and Cyber opportunities and challenges with you and your colleagues separately where we can provide individual support as appropriate. Please do let us know if this would be useful.

Naomi Horton
Partner, London
T +44 20 7859 1526
M +44 7826 927 962
naomi.horton@ashurst.com

John Macpherson
Partner, Sydney
T +61 2 9258 6479
john.macpherson@ashurst.com

Amanda Ludlow
Partner, London
T +44 20 7859 1294
M +61 401 557 750
amanda.ludlow@ashurst.com

Rhiannon Webster
Partner, London
T +44 20 7859 3070
M +44 7917 005 541
rhiannon.webster@ashurst.com

Matthew Worsfold
Partner, London
T +44 20 7859 1006
M +44 782 3340 980
matthew.worsfold@ashurst.com

ashurst.com

Design R013626 Apr 25