Cyber-security in the rail industry

Digitalisation of the rail industry is progressing at a steady pace, as stakeholders seek new opportunities to improve their efficiency and customer experience

From a passenger perspective, we have seen the digitalisation of ticketing systems enabling customers to buy and download tickets using their smart phones, making the passenger experience smoother, faster and easier. When it comes to infrastructure, Network Rail in particular has been investing heavily in modernising the railways, with an eye to improving capacity and reliability across the network. These advances make railway networks more interconnected and dependent on digital technology, but from a cyber-security perspective, it has also increased the possible threats to rail networks.

New EU legislation, in the form of the Security of Network & Information Regulations 2018 in the United Kingdom (the NIS Regulations) and the EU General Data Protection Regulation (the GDPR), has certainly forced participants in the rail industry to take heed of the cyber security risks that face the industry. High-profile cyber-attacks targeted at the rail industry have also highlighted that these threats are very real.

> ETCS works to ensure that a train does not exceed a safe speed and remains a set distance from other trains on the network. The intent is to increase train safety, capacity on the network (due to reduced minimum headway between trains) and improve punctuality

Eschewing digitalisation is not an option. Not simply due to the competitive advantages gained from improving systems and processes. Continued use of legacy technology can be costly as they become increasingly obsolete. However, failing to address the cyber-security risks that face the rail industry could have wide and serious repercussions.

Digitalisation and cyber-security

Digitalisation of the rail system is set to deliver much-needed improvements, including increased capacity and greater efficiency. One particular proposed improvement is the move to the European Rail Traffic Management System (ERTMS) and the European Train Control System (ETCS). ERTMS is intended to establish an interoperable rail framework across Europe, and will make use of ETCS, essentially a system allowing computers to communicate with each other to give the 'green light' for a train to proceed. ETCS works to ensure that a train does not exceed a safe speed and remains a set distance from other trains on the network. The intent is to increase train safety, capacity on the network (due to reduced minimum headway between trains) and improve punctuality.

Along with these advantages come increased threats. The risk of malicious third parties hacking into ERTMS cannot be ignored, and care needs to be taken to ensure that cyber-security requirements are appropriate to defend against potentially significant disruption to the rail network if ERTMS is compromised in any way.

Cyber-security risks

In 2016, the DfT advised that the threat of cyber-attacks on rail systems was increasing as a consequence of the industry's growing reliance on computer-based technology. This is particularly relevant for those systems that can be accessed remotely through public and private networks. Systems that can be accessed remotely can increase the risk of intrusions, and since 2016 we have indeed seen TOCs business systems falling victim to


Kulraj Badhesha


Anita Basi


Darren Fodey

cyber-attacks by malicious third parties.

In May 2017, as well as disrupting NHS hospitals across the UK, the WannaCry ransomware attack targeted Russian Railways and the German rail operator Deutsche Bahn. Deutsche Bahn train information monitors displayed the hackers' demands for money in return for unlocking the systems. In April 2018, Great Western Railway found that around 1,000 of its passengers' details had been compromised by hackers. According to security experts, the Wannacry virus spread through systems that still used the Windows XP operating system, which had long-since ceased receiving mainstream support from Microsoft. This acted as a wake-up call for many to upgrade their systems.

In these cases, we can only speculate on the hackers' exact motives for targeting the railway. Perhaps the intention was to inflict reputational damage due to political or commercial interests. Perhaps the acts were carried out for the hackers' personal satisfaction. Or maybe the intention was to steal personal data for the hackers' own financial gain. Malicious cyber-attacks on systems used in rail infrastructure could have far more serious implications though, including danger to life.

The threat of cyber-security risks does not only stem from malicious third parties. Computerised rail systems are also at risk from human error, such as failures to update and configure software correctly. This includes actions as innocuous as attaching unauthorised devices to networks. Each of these may also expose, or introduce, vulnerabilities allowing third parties to obtain remote access to systems.

Potential implications of cyber-attacks

Timetabling glitches and service interruptions caused by cyber-attacks could, at a minimum, disrupt commuters and cause chaos on the rail network. Signalling or power breakdowns could equally cause travel disruption and, at worst, danger to life although many levels of resistance are built in so the risk, we hope, is remote. From the perspective of a TOC, the implications of a cyber-attack could be far reaching – including reputational damage, loss of customers' personal data, the requirement to compensate passengers affected by the disruption.

There could also be serious financial and regulatory repercussions. TOCs are likely to be subject to stringent obligations under their franchise or concession agreements to provide a minimum level of performance. Timetabling glitches and service interruptions could therefore result in financial penalties becoming payable. Persistent breaches of performance requirements due to service issues and interruptions could ultimately lead to the termination of a TOC's franchise or concession. TOCs may also be subject to regulatory enforcement action, including non-compliance penalties from regulators. This might include the Office of Rail and Road in their capacity as safety regulator, and the Information Commissioner's Office in its capacity as competent supervisory authority under the GDPR.

TOCs are also considered 'operators of essential services' (OESs) under the NIS Regulations. This means that they are required to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential services rely. OESs are also required to take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of both the network and information systems used. This is to ensure continuity of those essential services. Any incidents which have a significant impact on continuity must be notified to the designated competent authority. In practice the DfT still expects rail operators to voluntarily notify the DfT of incidents before they have met the 'significant impact' threshold.

Failure to comply with these obligations may result in an enforcement notice. This could lead to a financial penalty if an OES fails to take steps to rectify a failure within a specified time period or if the competent authority is not satisfied with representations made by the OES. The prescribed limit for monetary penalties is £17 million where there has been a material contravention of the NIS Regulations.

> The threat of cyber-security risks does not only stem from malicious third parties. Computerised rail systems are also at risk from human error, such as failures to update and configure software correctly

Addressing increased security risks

The age-old adage that 'prevention is better than cure' can be applied to cyber-threats in the rail industry. When implementing new technologies and systems, cyber-security measures should be considered from the outset to ensure resilience. Multi-layered security measures (otherwise known as 'defence in depth') are recommended, making it harder for hackers to disrupt a system if a vulnerability in one measure is exposed and exploited. For incumbent systems, and to address future cyber-security risks, it is important to have robust risk management systems in place. This is to ensure that risks and vulnerabilities are identified by regular testing, actions are taken to protect systems and maintain security measures, and that any unusual behaviour is recognised and investigated.

Complex supply chains also expose TOCs to cyber-security risks, particularly given the increased information exchanges that takes place. As well as carrying out careful due diligence on suppliers and their security practices, TOCs would be well advised to include provisions in their contracts to minimise the threat of such risks and to ensure a joined-up approach to cyber-risk management across the supply chain. These can also help address TOCs' obligations under the NIS Regulations by (for example):

- including obligations to put in place (and periodically review and strengthen, as required) an appropriate cyber security management plan which allows for regular vulnerability scans and penetration testing using independent testers, to ensure that the TOC is poised to respond to any potential risks
- ensuring suppliers have appropriate training standards in place for their personnel and that employees are appropriately experienced so as to ensure that they are able to recognise and deal with any security risks presented to them
- ensuring effective business continuity plans are in place and ready to be implemented if services are compromised by a cyber-security breach – including, for example, a detailed procedure for steps to take in the event of a breach of security
- including notification obligations in the event of an incident that has a significant impact on the continuity of essential services.

Finally, given that railway networks are increasingly interconnected, there is a growing need for cyber-security approaches to be aligned across all participants in the rail industry across numerous jurisdictions. Cyber-security is a threat to the entire sector, and all industry players need to work together to harmonise their cyber-security activities and implement measures to address this constantly evolving threat.

Conclusion

As events of recent years have shown, with the growing digitalisation of the rail networks, cyber security is an issue that the rail industry simply cannot afford to ignore. Failure to implement robust security measures and practices could have, at worst, fatal consequences. Together with the high financial risks of suffering a cyber-security breach and the implementation of the NIS Regulations and the GDPR, cyber security should be near the top of everyone's agenda.

To address the increased threat landscape, it is crucial to understand rail systems, their vulnerabilities and the cyber-security risks that face them, and seek to tackle these by way of appropriate measures. Supply chain management is also key to ensuring that systems are resilient to attack - after all, you are only as strong as your weakest link.

Anita Basi and Kulraj Badhesha are Associates at law firm Stephenson Harwood LLP