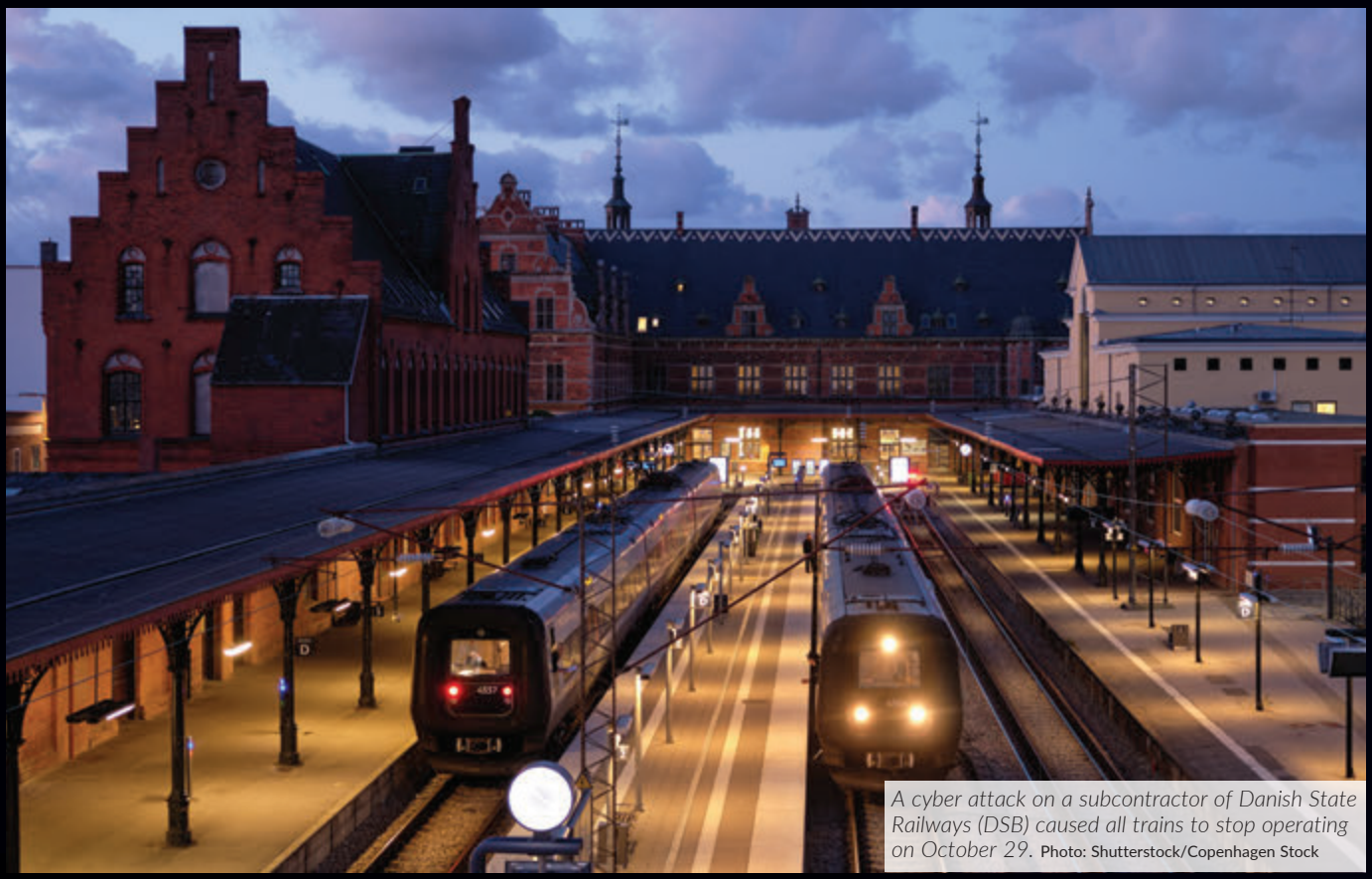
Rail's digital vulnerabilities worry cyber experts



A cyber attack on a subcontractor of Danish State Railways (DSB) caused all trains to stop operating on October 29. Photo: Shutterstock/Copenhagen Stock

As the rail environment becomes ever more digitalised, it is also becoming more vulnerable to cyber attacks that can range from efforts to steal data to malicious acts to disrupt operations. But rail's ability to deal with these threats is concerning experts, as **David Burroughs** reports.

ALL it took to stop trains operating in Denmark at the end of October was a suspected ransomware attack on a digital testing environment used by a subcontractor of Danish State Railways (DSB), the largest operator in Denmark.

DSB itself was not the target of the attack on the morning of October 29. Instead, the hackers hit Supeo, a supplier of asset management solutions to operators, infrastructure managers and passenger transport authorities. Supeo shut down its systems in response to the attack, train drivers could not use the Digital Backpack 2 software which allows them to access operationally critical information using an iPhone or iPad. As a result, all trains were brought to a halt, with local services unable to resume until 13.00 that afternoon. Long-distance services did not recover until the following day.

The cyberattack was not the first to disrupt rail operations and will not be the last. As rail becomes more digitalised, it opens itself up to more attacks if more isn't done to protect operational technology (OT) and supporting information technology (IT) systems.

In March 2022, hacktivists in Belarus reportedly disrupted some of the country's rail services after breaching computers that control train movements. The move by the group Cyber Partisans was an attempt to slow down the movement of Russian soldiers to Ukraine in the early stages of the war.

The hackers claimed to have put the network into manual control mode to "significantly slow down the movement of trains, but not create emergency situations." Specifically, points became inoperable after the hackers compromised systems by encrypting stored data, disrupting train movements in Minsk, Orsha and Osipovichi. Additionally, numerous websites linked to Belarus's rail network also showed error messages, making it impossible to purchase tickets.

That same month, the IT systems belonging to Italian State Railways (FS) and its subsidiaries Trenitalia and Italian Rail Network (RFI) suffered a major ransomware cyber-attack which disrupted ticket sales at stations, passenger information screens at stations, and affected tablets used by railway staff.

As a precaution, Trenitalia blocked the accounts of some passengers and shut down many of its IT services including ticket sales at stations, although passengers were still able to buy tickets online. Passengers who had not been able to purchase tickets were allowed to buy them onboard without penalty.

To highlight the scale of the threat to the rail sector from cyberattacks, the European Agency for Rail (ERA) and the European Union Agency for

Cybersecurity (Enisa) jointly hosted the second ERA-Enisa Conference on Cybersecurity in Railways in the French city of Lille on December 1 2022.

"When we look at the railway sector [compared with] other transport sectors, specifically aviation, rail is still showing lower levels of maturity, despite undergoing a major transformation due to the digitisation of OT and IT systems and infrastructure," Enisa executive director, Mr Juhan Lepassaar, told delegates. "For us, rail is a priority sector for two reasons: you are critical, but you also still have a way to grow."

ERA's executive director, Mr Josef Doppelbauer, cited the cyberattack in Denmark as an example of how an attack on a small supplier could have an important knock-on effect on the rest of the network, emphasising that rail is "exposed in several ways."

"We currently see an evolution of the railway system and of course this will change the exposure to cyber risks. We know that in order to be effective at fighting cybersecurity threats, we need a European approach, and we also know that there is a growing interdependence of the sectors."

The conference built on a four-year collaboration between ERA and Enisa as well as work within the sector. Such was the demand for places that organisers are planning an online webinar for those who were unable to attend in person.

Threat landscape

Enisa has produced the Transport Threat Landscape report, which is due to be released this month, and Lepassaar presented some early insights at the conference.

Enisa observed an increase in cybersecurity incidents in 2022 and this trend is expected to continue, with the Russian war in Ukraine changing the threat landscape. The main actors in the transport sector are cyber criminals, especially ransomware groups, who are motivated mostly by financial gain and account for 47% of incidents. Another group are hacktivists motivated by causing disruption and panic, accounting for 20% of attacks.

Prime threats appear to be ransomware, data theft, malware, and phishing. Enisa says that following the significant increase in hacktivist activity after the Russian invasion of Ukraine, instances of distributed denial-of-service (DDoS) attacks are on the rise and this trend is highly likely to continue. Rail IT rather than OT systems are more likely to be targeted. Enisa has also noted the prevalence of operational disruption caused by a reliance on systems that form part of the internet of things (IoT).

Mr Alex Patton, rail technical lead for transport practice at cybersecurity consultancy NCC Group, says another threat is how easily the rail environment can be accessed. "You only need to look at the wonderfully detailed pieces of graffiti we get on the sides of trains to know that the railway is an accessible environment," he says. "There are some things we can do to better prevent unauthorised access, but perhaps what is more important is detecting when unauthorised access may have occurred and when it could have led to tampering."

> When we look at the railway sector [compared with] other transport sectors, specifically aviation, rail is still showing lower levels of maturity, despite undergoing a major transformation. Juhan Lepassaar

Increased connectivity through new services like passenger Wi-Fi or integrated traffic management can make networks more exposed, and attack paths can open if the interfaces with these services are not properly designed, says Patton, who was until last year the cybersecurity manager for contracts let under East Coast Digital Programme to install ETCS on the London - Edinburgh East Coast Main Line in Britain.

New policies

To respond to these emerging threats effectively, rail needs to take security as seriously as it takes safety.

"Security is a bit trickier because it's an evolving topic, it's not something that is very embedded in the mindset of the rail industry," says Mr Miki Shifman, co-founder and chief technology officer (CTO) of rail cybersecurity specialists Cylus. "It has taken time for safety to develop to the level that it is now… and I hope that security will catch up. Someone from the outside only needs one mistake to create damage while someone [working to protect the system] from the inside needs to protect the entire system and that can be quite a big task."

Two new policies in Europe have been announced to strengthen cyber security, both impacting rail.

The new directive on security of network and information systems (NIS2) was published in the Official Journal of the European Union in December. It is designed to improve cyber security risk management and introduces reporting obligations across areas such as energy, transport, health and digital infrastructure.

NIS2 aims to remove divergences in cyber security requirements and the implementation of cyber security measures in different member states. To achieve this, it sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each member state. It also updates the list of sectors and activities subject to cyber security obligations and provides remedies and sanctions to ensure enforcement.

The directive also formally establishes the European Cyber Crises Liaison Organisation Network,

EU-CyCLONe, which will support the coordinated management of large-scale cybersecurity incidents.

In the biggest change for the rail sector, NIS2 is now also applicable to the supply chain. Member states can also identify all railway actors as operators of essential services, so that they would be obliged to monitor and declare any cybersecurity incidents to the national competent authority.

The European Commission (EC) also published the draft Cyber Resilience Act (CRA) on September 15 2022, which aims to set common cybersecurity standards for connected devices and services. While existing internal market legislation applies to certain products with digital elements, most hardware and software products are not currently covered by any EU legislation on cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products.

The CRA proposes "cybersecurity by design" at a product level, managed through regulation. This would be required for the product to receive the "CE" certification. It will also be necessary to notify Enisa of a cyber incident, while manufactures would have to provide updates against vulnerabilities for five years.

Lepassaar says the introduction of the CRA is important to ensure all connections, products, devices and software services are secure.

"They form a part of the supply chain that enables critical service providers to deliver services," he says. "If every component in the supply chain is not secure, you are vulnerable. So, from the user's point of view, and the railway is a user of services, products, and connected devices, it is crucial that the CRA brings a minimum level of security across all of these products."

There has been some pushback from the industry against CRA, which argues that it already has its own safety frameworks in place and that including rail in the CRA will layer additional regulations on top of the certification that the sector already has in place.

The European Rail Industry Association (Unife) said the European rail supply industry was making a huge effort in cybersecurity, notably in standardisation through international standard (IEC) 62443 and Technical Specifications for Interoperability (TSI) 5701, and its migration to international level, and is already committed to assessing the level of cybersecurity risk of digital products.

> "Suppliers, vendors and operators need to work together to protect the existing installed base, because that's what is currently transporting passengers and goods. That should be a high priority for protection. Miki Shifman

Unife says its main concern with the EC's proposal is that it overlaps with rail's legislative framework, including cybersecurity provisions, leading to a double certification process. It is also concerned that the proposal does not consider rail's particularities such as:

- rail is a system of subsystems already covered in the rail regulatory framework
- the long manufacturing process of up to seven years, that interferes with and can cause a very negative impact with the proposed entry into force of the CRA legislative proposal
- the long lifecycle of rail assets, which are designed to last for more than 30 years, which is not aligned with the management of vulnerabilities time proposed in the CRA, and
- the definition of responsibilities is also very different in rail from what is proposed in the CRA, as ownership of a product or system is transferred from the manufacturer to the operator.

"The application of the CRA proposal as it is now would be detrimental for the European rail supply industry and for the rail sector," the association says. "As Unife, we call on the EC to exclude rail from the CRA and to discuss with rail how to reinforce the existing rail regulation from a cybersecurity perspective taking into account ongoing standardisation cybersecurity activities." Further discussions are due between the EC, ERA and the sector to agree on a way forward, which could include the drafting of railway-specific provisions for cybersecurity to be captured in a TSI or Common Safety Methods.

"It would be logical that existing safety frameworks will also be able, vis-à-vis the context of the CRA, to be used in order to guarantee security," Lepassaar says. "I think this goal is achievable within the proposal that the commission has put forward."

Responsibility

Regardless of how the legislation and directives develop, it is the railways which must take primary responsibility of the security of their systems and networks.

"Some operators have been under the impression that cybersecurity is mainly the responsibility of the supplier," Patton warns. "Consumers have become used to security-mature products like the iPhone, where security is highly managed by the manufacturer. The rail industry is a lot more complex. We've seen multiple cases where operators have not sufficiently considered security in the procurement of rolling stock due to this impression. They then find out too late that they have taken on far more cyber risk than they realised."

Patton says investment in cybersecurity should be based on the potential impact of a cyber incident

rather than implementation costs.

Engineering and procurement staff should also be given proper training on engineering security, while operators should include cybersecurity considerations in tender documentation with potential suppliers assessed on their security capabilities. This would put more pressure on suppliers to ensure that their products, software and services are compliant, safe and secure. Operators also expect suppliers to provide tools to monitor their systems to allow them to detect attacks and intrusions.

"There are different frameworks built specifically for the rail industry, like the technical specification 5701," Shifman says. "There is also work by IC group 63452 that is taking this technical specification and making it a global standard. The goal is to produce something that will be comprehensive enough to be used by suppliers and operators to evaluate and manage the cybersecurity lifecycle of their systems."

Legacy systems

Securing new systems is not enough: one of the biggest threats is the number of legacy systems already installed and in use across the rail network that have digital capability and therefore need to be protected.

"Suppliers, vendors and operators need to work together to protect the existing installed base, because that's what is currently transporting passengers and goods," Shifman says. "That should be a high priority for protection."

There are challenges to this, including costly modifications that can require re-engineering and new safety assurance. "But at the same time, there's a lot you can do to gain better visibility and monitoring of your network, and that can happen even without modifying safety cases and without changing the safety constraints of your system," he says.

The introduction of digital technologies is increasing rail's vulnerability to cyber attack, potentially putting mission critical equipment such as signalling at risk. Photo: DB/Volker Emersleben

With existing assets, the operator should first focus on building their configuration management maturity, Patton says. "From there, the security risks need to be understood with regular security assessments involving penetration testing to help identify system vulnerabilities. Particularly in rail, it's not always possible to eliminate vulnerabilities. As an operator builds maturity, implementing security monitoring provides an opportunity to detect and react to cyber incidents more efficiently."

Lepassaar says one of the biggest threats over the coming decades will be a shortage in skills. "Cybersecurity is becoming more and more embedded into different areas," he says. "But it also means that the level of expertise becomes harder to find - we will become competitors in the talent markets. I believe that the only way to overcome it is through collaboration and building synergies."

The sheer scale of the task, both in terms of costs and the work required, to secure the rail sector appears insurmountable. But this is essential work that can only be achieved through collaboration. It is also a task that will keep evolving as digitalisation progresses, including through the introduction of new systems and technology such as AI.

"There are always new aspects of digitisation so there are always going to be new aspects of security," Shifman says. "Industry feedback will feed the future generation of regulations or standards and, as an industry, we just need to keep working together. We need to keep evaluating the attack surface, evaluating the motivation of threat actors, and keep evolving and learning about what good security looks like in the rail environment." **IRJ**