CYBER-SECURITY

Thanks to advances in digital solutions and innovative technology, our railways are delivering better operational efficiency, reliability and enhanced passenger experience. However, with these advances comes the risk of cyber-threat. How is the industry reacting to challenges around cyber-security?

The growth of big data and cyber-threats

With the rise of big data and the subsequent growth in cyber-threats, *Tommaso Spanevello*, Public Affairs Manager at UNIFE, outlines an effective cyber-security strategy for the rail sector and highlights that more cross-industry collaboration is needed to ultimately benefit the future of rail's success.

DIGITALISATION and the spread of web-based technologies is profoundly changing communication patterns between businesses, organisations, communities and individuals. In this era of Internet of Things (IoT), an ever-growing network of objects, data, processes and people connect with each other using devices such as computers, tablets and smartphones. As IoT progressively becomes the 'Internet of Everything', such continuous inter-connection produces a rapidly expanding volume of created, transmitted and stored data. The importance of collecting, managing and effectively processing data is increasingly being acknowledged by the rail supply industry, and promises to deeply transform the rail sector's business-as-usual. Indeed, by harvesting and processing this data, we can derive actionable insights that will enable us to improve rail business results.

If, on the one hand, the effective management and processing of data would give rail companies the business intelligence to enhance performance and optimise strategies, it would also, on the other hand, expose massive quantities of sensitive and personal information to increase cyber-threats. As a matter of fact, the technological progress and the use of big data completely redefine the security environment as systems become more vulnerable to new types of threats.

The rise of big data in the rail sector and the evolution of cyber-security are, therefore, intertwined in many ways. UNIFE analyses this relation in its new Vision Paper 'Digital Trends in the Rail Sector', published in April 2019 and prepared by UNIFE's Digitalisation Platform. In the document, among other digital trends such as artificial intelligence and new mobility services, specific chapters are dedicated to big data and

Cyber-attacks may result in physical damage to crucial railway infrastructure such as signalling equipment

cyber-security. Understanding this relation can help any company to better determine what capabilities it must develop or acquire in order to take full advantage of the data they have as well as keep that data safe.

An effective cyber-security strategy for the rail sector

As aforementioned, digitalisation can indisputably contribute to making rail transport safer, more efficient and more convenient for both passengers and freight, but it also exposes rail systems to cyber-security risks. While rail harnesses the benefits of digitalisation and IoT, one can expect cyber-attacks to become ever-more sophisticated. Indeed, we must be aware that cyber-threats are as versatile and dynamic as the digital world and its applications.

> *“Digitalisation can indisputably contribute to making rail transport safer, more efficient and more convenient for both passengers and freight, but it also exposes rail systems to cyber-security risks”*

There are many different types of cyber-threats that could adversely affect rail transport systems. Some attacks may result in physical damage to crucial railway infrastructure such as the signalling equipment, while others might not even be focused specifically on the rail system (e.g. viruses and malware). Moreover, due to the complex landscape of potential threats, anticipatory measures are often difficult to develop and put in place.

Embracing the need for robust cyber-security measures and being prepared to deal with cyber-attacks represent significant challenges for the rail sector, both today and in the future. Contributing to an effective and robust cyber-security strategy is, therefore, a core objective for the European rail supply industry. Besides the aforementioned Vision Paper[1], our members have also been active in a dedicated ‘Cyber-Security Working Group’ which has recently prepared a technical paper identifying the main cyber-security-related challenges in terms of standards and technology – this technical document effectively complementing the messages included in the Vision Paper.

Granted, we can try to identify four main elements – among others – which would be crucial in devising a holistic and sound cyber-security chain in the rail sector:

1. Dedicated skills

The first step depends on understanding the cyber-risks and their potential impacts on the rail system. This must be done through developing targeted cyber-security-related skills and knowledge, as well as increasing the cyber-awareness regarding cyber-threats within each company and organisation. Therefore, cyber-security-related skills should be strengthened, especially regarding two dimensions: The detection of cyber-threats and the response to them in order to minimise the negative impacts of cyber-security incidents and enable a swift recovery of systems and services following any such incident.

2. Sectorial and cross-sectorial cooperation

In addition to developing critical expertise and filling any skills gaps, we strongly support the strengthening of cooperation among all the relevant actors in the rail sector – and beyond. The exchange of knowledge and the sharing of experience with other concerned businesses via existing networks – such as associations, platforms or governmental information forums – would enhance the capacity of rail stakeholders to develop and implement effective measures to protect their systems and services against cyber-threats. Notably, the importance of cooperation was strongly reiterated at the '1st Transport Cyber Security Conference' (organised by the European Commission and the ENISA Agency) in January 2019 in Lisbon. At the event, all the EU's Transport Agencies (ERA for railways, EASA for aviation and EMSA for maritime) pledged to strengthen cyber-security synergies between different modes of transport.

3. Security-by-design

Another crucial element for an effective cyber-security strategy stands in increasing the focus on security aspects during the design process of a product – thus giving them the required priority – and ensuring compliance with relevant regulations and standards at an early stage. As a positive consequence, products and systems that have been built with security in mind can help to spare time and resources, contributing to reducing the risk and avoiding the costs of an effective cyber-attack, avoiding the hectic and expensive replacement of a component.

4. Research and Innovation (R&I)

The fundamental role played by R&I in fostering the digitalisation of railways must also be highlighted. This is also true when it comes to new solutions which can enhance the cyber-resilience of rail. The 'Rail 2050 Vision'[2] by the European Rail Research Advisory Council (ERRAC) has 'Security' as a core element, highlighting that a robust ICT infrastructure, combined with strong business continuity processes, will ensure the high availability of the rail system and services. In particular, the rail sector's R&I commitments have found their gravitational field in the establishment of the Shift2Rail Joint Undertaking[3] (JU) under Horizon 2020. Regarding cyber-security, the Shift2Rail JU is currently working on a specific Technology Demonstrator aiming to achieve the optimal level of protection against any significant threat to the signalling and telecom systems.

A refocussing of rail-related R&I activities is needed for the post-2020 period – this is why UNIFE strongly called for the continuation of the Shift2Rail JU under the Horizon Europe Framework Programme. A 'Shift2Rail 2' will enable Europe's rail sector to develop various value-added products and services also in the field of cyber-security.

Working together with the EU institutions

While our sector, with the European rail supply industry at its forefront, is ready to engage in the establishment of an effective cyber-security strategy, the role and action of the EU institutions become as essential as ever.

Cyber-security, in the latest years, has been at the centre of the European legislative process. Notably, the Network and Information Security (NIS) Directive (EU) 2016/1148 – adopted in August 2016 – has marked the first step towards a more coherent and harmonised cyber-security management in Europe. Moreover, the EU cyber-security roadmap includes the establishment of a cyber-security competence network with a European Cyber-Security Research and Competence Centre and increasing the powers of the European Network and Information Security Agency (ENISA) through the so-called 'Cybersecurity Act' – adopted in December 2018. Eventually, another landmark piece of EU legislation which affects cyber-security is the General Data Protection Regulation (GDPR), introducing strict rules on how private information may be collected and managed. The main purpose of the GDPR is to further strengthen data privacy, and its introduction has led to the development of new cyber-security solutions – which would have to be developed in compliance with the new protection levels for data.

The European rail supply industry believe that the European Commission – with the key support of the European Parliament and the Council – should continue to develop a consistent and harmonised European legal framework and management system for detecting as well as addressing cyber-security risks. We consider it essential that fragmentation in the European cyber-security landscape is overcome both at institutional and industry levels. In this regard, strengthening the mandate of ENISA, turning it into a real 'EU Cybersecurity Agency', represents a positive step in the right direction.

Granted, the protection against cyber-threats is a vital element of maintaining a safe and reliable railway – with its complex interdependences and legacy infrastructure. The European institutions can count on the full commitment of UNIFE and its members in ensuring the integrity of rail systems and maintaining operational continuity standards.

TOMMASO SPANEVELLO is Public Affairs Manager at UNIFE, responsible for innovation policy, digitalisation and sustainable and urban mobility. Since January 2018, Tommaso has also been the Executive Secretary of Rail Forum Europe, the Members of the European Parliament's Association dedicated to rail transport. Prior to joining UNIFE, Tommaso was in charge of the policy department of the European Rail Infrastructure Managers Association (EIM). With a background in International law, Tommaso studied and worked in Italy, United States, Finland and Hungary.

REFERENCES

1. www.unife.org/component/attachments/attachments.html?id=1011&task=download
2. www.errac.org/publications/rail-2050-vision-document
3. www.shift2rail.org