‘Good guys’ must work together to keep rail networks **cyber safe**

As Europe’s rail networks become more digitalised and the tactics of cybercriminals evolve, UNIFE Director General, ***Enno Wiebe***, says collaboration is the only the way forward.

As we see with the ‘bad guys’, their technological capabilities continue to evolve with the technology at their disposal.

AS EUROPE faces geopolitical uncertainty and our world becomes more digitalised, more opportunities for ‘bad actors’ arise. Whether they are hostile states, internal actors or criminal groups, they will take advantage of new and increasingly sophisticated technological methods to target vital systems and key infrastructure.

For railways and rail systems, there are many elements of security where we must remain vigilant. We have seen ticketing, payment and communications systems targeted, underscoring the need to have a holistic approach in building security systems.

One of the fundamentals of a secure system, is in the products themselves – the components, the hardware and the software. A key, well-rounded response involves empowering companies designing the latter, as it is a central part of the process in designing ongoing patches and updates.

As we see with the ‘bad guys’, their technological capabilities continue to evolve with the technology at their disposal. Whether this is utilising artificial intelligence to enhance their malware, ransomware and phishing opportunities, they will continue to perfect their techniques.

We need to ensure that there is the creation of a chain of information where all stakeholders – from operators to infrastructure managers to manufacturers – freely share information and remain involved in the process. This will ensure a higher quality and level of security for railway systems.

Further to this, we need sound frameworks of regulation and standardisation, in order to ensure our sector can work to produce the best possible products to protect European railway networks.

The European Commission’s Cyber Resilience Act (entered into force in late 2024, and applicable from late 2027) is the beginning, but its implementation and interpretation is crucial. We are a proud member of the European Commission’s Cyber Resilience Act Expert Group, which is vital in advocating for clear guidelines for implementation of the text.

Enno Wiebe

Enno Wiebe is the Director General of UNIFE. After completing his civil engineering studies at the University of Applied Sciences in Dresden, Germany, and the University of Cape Town, South Africa, he began his professional career at Deutsche Bahn. From 2007 to 2011, he worked at the International Union of Railways (UIC) in Paris, France. Before being appointed to UNIFE, Enno Wiebe served as the Technical Director of the Community of European Railway and Infrastructure Companies (CER), where he oversaw the technical domain, and other related policies and projects.

UNIFE, together with the railway and urban rail operating community of CER, EIM and UITP, are also collaborating separately as a dedicated Cyber-security Rail Sector Group, to seek further guidance from the European Commission on a range of key details. Among these concerns are clarifications on reporting obligations, relevant technical support periods and due diligence, as well as the questions of risk assessment and the question of liability on open-source projects.

As part of this rail sector working group, we need to work to ensure, through different avenues, that the topics from the legislation (with limited guidance from the Commission at this stage) are addressed – such as system extensions and the relationship the legislation has with vehicle authorisations.

Other outstanding issues without guidance from the Commission include the classification of products which should or should not be subject to CRA requirements, and how to successfully balance the legislative implementation with current European interoperability requirements.

Further to this, it is important to address the clear issue of skills. Europe has a shortage of cyber-security professionals. These are across many different roles, from producers of cyber systems, technicians and even policy experts.

According to an assessment from the International Information System Security Certification Consortium (ISC), Europe faces a deficit of over 347,000 cyber-security professionals. In France for instance, a shortage of nearly 60,000 cyber-security experts was estimated in 2023.

To mitigate and minimise these cyber-security risks to railways, we need to ensure the ‘good guys’ are ready and can collaborate. There’s a lot of work to do, and now is the time to make that happen.