Operational cyber security – the future is digital

Emma Taylor, Head of Digital Safety at RazorSecure, writes about the importance of cyber security

The Williams-Shapps Plan for Rail has put into motion a new approach for the rail industry, fundamentally shaking up its its structure, accountabilities, and delivery mechanism. It is the biggest recalibration of our industry since privatisation, which we must view as a watershed moment, setting us on track for a new era.

Central to making this new era a success will be an understanding of how the world has changed around us. Digital systems are embedded on all our trains and have helped improve efficiency and the passenger experience. But as we embrace digital opportunities, we must also consider how we can safeguard our digital systems – maximising their potential and minimising any risks.

The benefits of cyber security

This is where operational cyber security enters the story. The UK has an exemplary safety record and excellent processes in place when it comes to the physical railway. We have systems in place to prevent faults with equipment, derailments and collision. But in the digital space, our emphasis on safety and security is far less established, in part because our shared knowledge and understanding is less developed.

Digital moves more rapidly and is less predictable, meaning the past can't be used to predict the future.

As we move towards greater efficiency, more deployment of digital systems, and greater streamlining and integration across the industry, it's essential our understanding of how things connect improves if we are to ensure the safe running of the railway.

There are pockets of excellence using cutting edge technology, but most train operating companies are currently running without a holistic approach to cyber security in place. But software, like hardware, can fail. It can also be a target for hostile or unintended acts which increase risk.

As our systems become more digitised, they also become more complicated, interconnected and vital to services running smoothly.

It is here where cyber security provides rail operators with continuous monitoring and asset management, so that problems with digital systems are identified to keep them working in an optimal way.

Moving to a prevention rather than cure approach would stop delays and cancellations, thereby enhancing passenger experience.

At present, the diagnostic process often takes far longer than actually resolving a fault, because most fleets lack the diagnostic capability to properly investigate a cyber security incident.

Finding fault

Afterall, when something goes wrong physically, it is easier to spot. If the doors are not closing or a signal has stopped working, that is obvious.

But in the increasingly complex web of interconnected digital systems, a fault is often very hard to identify unless you have appropriate monitoring and analysis in place. This is crucial not just for passenger safety, but also for maintaining and building passenger trust.

> Moving to a prevention rather than cure approach would stop delays and cancellations, thereby enhancing passenger experience

Punctuality and reliability are the basics we must get right if we are to create the modern, responsive, reliable and comfortable experience as set out in the Williams-Shapps Plan for Rail.

Developing a deep knowledge and understanding of how our systems work so we can anticipate faults and fix them before they impact our customers, is not just a 'could do' but a 'must do' if we are to make this ambition a reality."

As well as our systems being more digitally integrated, our rail industry is set to be more closely integrated than it has been in decades.

We have the opportunity to take a whole system approach to the sector. Our regulatory framework is provided by the Office of Rail and Road (ORR) and Department for Transport, supported by the National Cyber Security Centre as Technical Authority. The guidance is already in place – ORR's RM3, Networks and Information Systems Cyber Assessment Framework and TS50701 – to help shape our approach to the digital parts of the railway.

The way ahead

With much still in flux about the future of the industry, one thing we can predict is that cyber threats will continue to grow.

The rail industry must move quickly to enhance and protect our digital systems, ensuring that the new era of rail is robustly future proofed and ready to embrace the challenges of operating in a digital world.