ON CYBER ALERT

Britain's railways have a proud record as one of the safest and most intensively used networks in the world, but difficult challenges are ahead to maintain this performance as the adoption of new technologies creates new risks, warns RSA

Delegates learn more about the changing risk environment prompted by the digitalisation of rail systems, at RSA's fourth annual rail forum at London Transport Museum on November 3. RSA.

The rail industry is in the middle of a digital revolution that is having an impact on every aspect of railway operation.

In order to optimise costs and efficiency, and improve the passenger experience, significant technological advances are being made in fields such as smart ticketing and remote asset condition monitoring. Meanwhile, network capacity is set to be increased by European Train Control System (ETCS) in-cab signalling under Network Rail's Digital Railway programme.

But with the more widespread use of digital technologies comes a new set of risks, as the software and communication systems they rely on become vulnerable to cyber-attacks.

The potential size of this risk has been laid bare in other sectors such as the National Health Service, which was left paralysed in May by the high-profile spread of a computer virus called *WannaCry*, when the 'ransomware' was unwittingly released into its internal systems by a member of staff having been delivered by email attachment.

In light of recent attacks, insurance company RSA is making train operating companies and other railway systems providers more aware of these threats, and how they can be mitigated from a risk management and insurance perspective.

On November 3, RSA held its fourth annual rail forum at the London Transport Museum, where delegates heard from expert speakers from organisations including RSA, Network Rail and the Rail Delivery Group.

NR's Chief Cyber Security Officer Peter Gibbons said: "This issue is not about digital products or services, it's about a new way of thinking about problems and how we address them. After all, we are not the only industry that has looked to digital technologies to solve problems.

"It will mean a big change to the risk landscape, as having digital systems that are faster and have more capacity is great when things are good, but you also have the same speed and scale when things go wrong, so we must be prepared."

Gibbons added that particular problems in risk management will be caused by the interdependence of discrete technologies that are operated by different parties but must work in unison - for example, track circuits and GSM-R communications masts that are operated by NR, and in-cab signalling equipment which relies on them.

He said that full co-operation will therefore be needed between system operators in order to provide robust protection from cyber-attacks, which make no such distinctions in ownership.

"When everything is connected it creates its own challenges. We don't own all of the systems, so you get multi-tenancy problems. When ETCS is in cabs, who owns it - Network Rail, the train operator or the rolling stock owner? How are you going to manage cyber security when the end user device is divorced from the data source?

> "It's not enough to protect your own devices and systems, we need to think about the wider supply chain."
>
> **Peter Gibbons,**
> ***Chief Cyber Security Officer, Network Rail***

"If we don't challenge the risks together, no single entity can do it and we will fail. It's not enough to protect your own devices and systems, we need to think about the wider supply chain. We no longer have to just manage our own infrastructure and systems."

Gibbons added that success would also come from structural changes where the purpose of IT staff is no longer treated by companies as purely a support function, but as part of the core business.

In the meantime, strong business contingency planning is needed so that measures are in place to keep systems operating when they have been breached. Gibbons said that organisations must be able to respond rapidly in order to limit reputational damage and retain public confidence - especially important in an age of social media where delays can be rapidly broadcast by passengers over the internet.

"We don't just have to protect our systems, we have to let the public know we're doing it, too. For businesses to thrive they must recognise the need to adapt to the new reality, and think hard about how we view our technical teams and customers.

"At NR, we have a security reference model with three strands: deter, prevent, and asset protection. It's not realistic to think that we won't ever suffer an incident, so we must be able to detect an attack and have an incident response that segments networks to limit damage. It's not all about building a big wall, but having a response."

Mark Newton, head of policing security at RDG, repeated the need for pan-industry co-operation, especially as the perpetrators of cyber-attacks are often more difficult to locate than in traditional crime.

He pointed to the RDG's Cyber Security Strategy, which has been designed to achieve just that.

He added: "Can we afford to treat cyber threats as an IT issue, a project issue, or a leadership issue? We are not going to be able to arrest our way out of this, and many of the criminals are beyond the reach of justice.

"We have to put in preventative systems and recognise that there is a capability gap that needs to be filled. The risks are high but manageable if a new approach is taken, and this becomes a leadership issue."

Without adequate protection against cyber threats, the cost of repairing compromised systems and replacing damaged equipment can be considerable.

According to RSA Global Transportation Specialism Leader Steve Medhurst, commercial insurance solutions are increasingly available from providers such as RSA, as businesses take the risks more seriously and want to take the necessary steps to protect themselves.

> "Cyber-attacks can potentially be as disruptive as physical perils such as a train being stopped by a signal failure."
>
> **Steve Medhurst,**
> ***Global Transportation Specialism Leader, RSA***

He says: "In the past, not enough was known about cyber risk and the exposure attached to it.

"However, both client and insurer knowledge of cyber risk has improved, and there is now a recognition that IT must be more joined up with the rest of the operational business. Employees play a significant part in helping with cyber risk identification and prevention.

"A risk management approach will continue to inform exposures, and improve disaster recovery and communications plans, which are critical for the protection of a client's reputation and business operations in the event of a cyber security breach.

"Insurance plays a significant role in any solution as it can provide immediate and relevant responses such as IT forensics, legal services, incident management and communication specialists, in addition to working with clients to provide preventative risk management services." ■