STEPHENSON HARWOOD

June 2022

Stay on track: Cyber security risks in rail sector

The increasing cyber threat

The level of cyber crime continues to grow at an unprecedented rate in the UK and across the globe, with UK Government figures from a DCMS 2022 survey showing that nearly 40% of businesses surveyed had suffered cyber security breaches or attacks in the last year. Over recent years the threat of attacks has been exacerbated by the increase in staff working from home, from increased political tensions and activity from hostile states.

Ransomware continues to be a focus of cyber criminals and is now the most prominent and immediate cyber threat to rail businesses. If it isn't already, this now needs to be a top priority for rail businesses.

There have been high-profile examples in the news of cyber attacks on railway companies which have even led to services being temporarily suspended. Ransomware attacks have also targeted self-service ticket machines and the sale of tickets at ticket offices which has led to significant disruption.

In this latest insight we look at why rail businesses are particularly exposed, the regulatory landscape, and cover the technical and practical ways that organisations can prepare for, and plan their response to, a cyber-attack.

Key takeaways

- The current threat level is high and the rail industry is a likely target.
- Supply chains within the rail industry often create the most material vulnerabilities.

Key actions

- Audit and test technical security measures.
- Review, refresh and test response plans.
- Map, audit and test supply chains.
- Produce a "grab sheet" with key information on a couple of pages.
- Engage third party professionals – forensic IT and legal – so they are available in an emergency.
- Refresh training to key stakeholders.

Key target

Rail businesses are at a heightened risk of attack from cyber criminals for several key reasons, including:

- they hold a significant amount of valuable and sensitive data (including personal data and operations data) – this can be sold by attackers on the black market or encrypted as part of a ransom request;
- advanced technology is often combined with unsupported legacy technology in rail management systems – this means systems and integrations can be more vulnerable;
- rail is critical infrastructure with cyber attacks likely to cause significant disruption – the risk of reputational damage caused by attacks can drive up ransom demands and make them more lucrative;
- systems are increasingly integrated to monitor the conditions and movements of trains – vulnerabilities in these systems could be exploited and the impact of an attack could be devastating; and
- communication between different operational teams can be fragmented in the rail sector – this can lead to operational vulnerabilities and a disjointed approach.

It is important to understand that Cyber criminals are now "professionals", undertaking their own detailed research on which organisations and sectors to attack, and so they will be aware of these factors and how to exploit them.

What is at risk?

Cyber security breaches or attacks carry a number of risks to the rail industry, including:

- data loss – sensitive personal and financial data could be exposed to third parties;
- business interruption – systems could be corrupted, or encrypted beyond use;
- extortion – ransomware attackers request payments for de-encrypting data and systems;
- additional expense – breach remediation can be costly and a drain on internal resources;
- exposure to regulatory fines – fines are possible for breach of legal obligations;
- reputational damage – adverse publicity can be damaging; and
- legal claims - individual and group actions could be brought.

What is the industry doing?

The Department for Transport ("**DfT**") has issued Rail Cyber Security Guidance focussing on rolling stock and infrastructure cyber security principles. With the introduction of European Train Control System "in cab" signalling relying on computers interfacing with each other, rather than traditional colour-light signals, this is vital. Principles include "if it is not secure, it's unlikely to be safe", ensuring responses are proportionate and targeted and that systems are designed to be secure. The importance of effective training is highlighted and practical examples are given such as emergency braking being "hard wired" and passenger wifi systems being physically or electronically separate from train control and signalling. Of course, the overriding factor in the guidance is the safety of people.

Partly in response to the DfT's guidance, the Rail Delivery Group published its Rail Cyber Security Strategy in January 2017. The strategy's key principles are:

- **understanding** the cyber security risk to the railway and the potential impact of a cyber security incident;
- **protecting** assets by safeguarding the confidentiality, integrity and availability of information and systems and taking steps to deter incidents;
- **detecting** abnormal behaviour in people, assets or technology, promptly raising alerts and sharing information; and
- **responding** in a way that reduces the impact of cyber attacks and reporting to improve threat intelligence and protection.

These principles are supported by a series of objectives, activities and actions at all levels of detail to better protect the industry from the external threats it faces.

Regulatory and contractual requirements

1. Railways Act 1993

The Secretary of State for Transport has broad powers under the Railways Act to issue instructions to anyone who owns or operates a railway asset or provides railway services to protect people from "acts of violence". As well as requiring information to be provided and plans to be prepared, any instructions can compel asset owners or operators to take particular steps, which may include modifications to assets or associated equipment or apparatus. It is a criminal offence not to comply with any such instruction without reasonable excuse, with a risk of imprisonment if convicted. These powers are broad enough to capture cyber attacks and we understand the DfT regularly works with the industry to implement proportionate measures in this area.

2. National and Information Systems Regulations 2018

The Network and Information Systems Regulations 2018 ("**NIS Regulations**") apply to operators of essential services, including operators of certain railway assets. The NIS Regulations impose obligations on such organisations to take appropriate and proportionate measures to ensure the security of network and information systems and to notify competent authorities of security breaches. For the purposes of the rail sector, the DfT is the designated competent authority.

Incidents which have a significant impact on the continuity of essential services must be notified to the DfT, although in practice there is an

expectation of notifying the DfT of incidents before they have met the 'significant impact' threshold.

Sanctions for non-compliance apply on a sliding scale, with maximum penalties ranging from £1m to £17m depending on the nature of the contravention.

3. Cyber Assessment Framework

Consideration of the Cyber Assessment Framework published by the National Cyber Security Centre ("**NCSC**") is essential. It is a tool for assessing cyber resilience and consists of 14 principles which are written in terms of outcomes. Rail businesses will have to establish how these principles apply to their rolling stock and signalling systems.

4. UK / EU General Data Protection Regulation

Compliance with obligations under relevant data protection laws is key, including the obligations under the UK/EU General Data Protection Regulation ("**GDPR**") to have clearly documented policies and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This is a broad obligation and imposes duties to ensure both internal and external systems are robustly protected.

In the event of a cyber-attack, rail businesses (and potentially other connected data controllers affected by the breach) must report any personal data breach to Information Commissioner's Office, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned. In some instances, rail businesses must also communicate the personal data breach to the data subjects such as customers and employees, and an incident may be reportable even if data is not extracted or publicly released – unauthorised access to personal data constitutes a personal data breach under the GDPR and can trigger reporting obligations.

Penalties for non-compliance with data protection laws can be up to the greater of £17m/€20m or 4% of total annual worldwide turnover of the group.

5. National Rail Contract

For train operators under National Rail Contracts – which we assume will be the basis of future Passenger Services Contracts as well – there are a number of additional contractual obligations to:

- prepare and maintain an incident response plan setting out how an operator would respond to an emergency or incident, which includes cyber security incidents;
- share information on cyber security threats with the DfT, British Transport Police and the NCSC (see more below on this); and
- comply with cyber incident reporting guidance and using the NCSC Cyber-Security Information Sharing Partnership.

The main cyber security threats

Ransomware, a form of malware, is now the biggest cyber threat to most businesses. This malicious software is used to encrypt data/information and disable access to systems, so that cyber criminals can extort a ransom in exchange for the decryption key.

Typically, ransomware attacks are delivered through phishing emails (see below), that then enable attackers to gain access to the underlying network to deploy encryption software on the data assets. In combination with this, cyber criminals also often extract files and data that they can share with the target as proof of their control and access over the network. They also often threaten to release these files if the ransom is not paid.

This type of attack could paralyse most rail businesses, by disabling access to timetabling and ticketing systems, preventing business as usual transactions such as purchasing tickets, and threatening the security of customer personal data. An attack could also affect the operation of critical infrastructure, potentially putting lives at risk. As a result, businesses often face the difficult discission of having to consider paying the ransom demands, often in cryptocurrencies that are almost impossible to recover at a later date.

Other key threats include:

- **Phishing:** seeking to obtain information whilst appearing to be from a legitimate source or contact. These attacks can be used to target individuals (spearfishing) e.g., to appear to be a genuine email from a CFO requesting a revenue controller to make an urgent payment or to request sensitive payment details.
- **Hacking:** gaining access to systems via IT vulnerabilities to steal information, such as bank account details, or to obtain valuable intellectual property. There are also threats from hacking by individuals who hack systems as a "hobby", or to test and train their cyber skills.

- **Data leakage:** obtaining access to data and confidential information through vulnerabilities and unauthorised transmissions – these can occur through the sharing of unencrypted files, or backdoors on websites. Data leaks by internal personnel, both by error and maliciously, also pose a threat.

Supply chain risks

When considering cyber vulnerabilities, it is imperative that the analysis covers all potential supply chain vulnerabilities. Whether that is operating and joint venture partners, suppliers of internal systems, or other third-party service providers. These can often be easy and rewarding targets for cyber criminals, as gaining access to their environment may more easily allow access to multiple underlying end users.

In assessing and managing the supply chain risks, it is important to:

- document key contractual information, reporting obligations and contact details in an easily accessible format – in the event of a breach, it is vital to have this basic information readily to hand;
- ensure documented minimum-security requirements are kept under review to ensure they reflect industry best practice;
- maintain a dialogue with key suppliers to understand how they are taking action to mitigate evolving cyber risks;
- carry out security audits to ensure suppliers are complying with their security and data handling obligations,
- where relevant, carry out routine penetration testing on supplier systems and interfaces (or ensure suppliers carry out, and report back on, such testing); and
- include your key suppliers in your business continuity plans and get them to participate in continuity testing activities.

What should rail businesses be doing to implement appropriate security measures?

Rail businesses should ensure that they have access to expert internal IT resources, and where relevant external specialists should be engaged to assist with implementing, monitoring, and updating technical security measures.

As a minimum, ensure that the following security fundamentals are implemented:

- carry out regular (or ideally real-time) back-ups of systems and data and implement continuity arrangements for failover support;
- monitor the network to check for suspicious activity or unauthorised access - typically using endpoint threat detection and response (ETDR) software;
- disable the use of removeable media such as USB memory sticks or ensure that systems force scans on them for malware;
- limit access controls to highly sensitive data, information, and systems to only those that need access to fulfil their specific role;
- regularly test networks and systems for vulnerabilities and test the interfaces and data exchanges with third parties;
- ensure staff are trained on cyber security, have read, and understood policies on the acceptable use of IT, and are aware of their own obligations to maintain the security and confidentiality of information and data assets and to report any potential breaches; and
- monitor key threats and updates, such as from the National Cyber Security Centre who publish threat reports and provide other excellent resources and services.

Those responsible for implementing security controls should ensure that any off-site networks and servers, such as at warehouses, regional offices and manufacturing sites (that may use standalone IT systems) are included within the scope of any cyber security measures.

Cyber incident response planning

It is almost impossible to quickly respond to, and mitigate the effect of, a cyber security breach or attack if you do not have adequate response processes and tools in place. However, the temptation is often to produce lengthy, detailed, policy documents and response plans. These can be useful reference points when checking security requirements or supplier assurance steps during a procurement process, but they aren't necessarily helpful on a Friday afternoon when an incident comes to light (and in practice, can be so cumbersome they are totally disregarded).

From our experience, to supplement any detailed policy document, organisations should ensure that they have a short "grab sheet" of no more than a couple of pages that documents the key

information. This should set out contact details of who forms the initial response team - including details of external third-party specialists, such as forensic IT consultants and legal advisors – and a prioritised checklist of actions to initiate. This will ensure that the "first responders" can be mobilised quickly, and critical containment activities can be implemented without delay.

Bringing all of this together, set below are our top tips for incident response planning:

- produce a grab sheet, keep it updated, and keep it to hand;
- set up notification email addresses – one for reporting potential incidents, and one to cascade internal notifications;
- build a good relationship with an IT consultancy business that can deploy forensic IT specialists at short notice to assist with initial investigations and containment activities;
- engage external legal counsel on a retainer – you need to know a trusted legal advisor who can step in and support on critical incidents (and you don't want client/matter onboarding admin to delay their ability to respond and advise);
- ensure you understand any legal reporting obligations, such as to the DfT, British Transport Police, Information Commissioner's Office (and other relevant regulators), including applicable timescales;
- raise awareness of cyber risks across the organisation by ensuring everyone has participated in relevant on-going training; ensure key stakeholders, and in particular those listed on the grab sheet, are trained on handling a cyber incident; and
- understand the terms of any insurance cover, including any breach notification requirements (which should be noted on your grab sheet).

We are here to help

Cyber risks will continue to evolve at a rapid pace, and the risk levels in the UK are likely to remain high for the immediate future. Rail businesses must maintain their resilience to cyber-attacks, and ensure that their internal controls, governance, and planning are up-to-date and fit for purpose.

Should you wish to discuss any of the matters raised in this insight, or require assistance with reviewing and updating your organisational cyber security measures and response plans, please contact one of our experts and we will be happy to discuss further.

Our cyber security services

- Policy reviews and updates
- Supply chain audits and risk mapping workshops
- Regulatory guidance
- Bespoke training sessions
- Response planning – grab sheets and containment plans
- Incident management
- Advice on regulatory notifications

Contact

Simon Bollans

Partner, Commercial, Outsourcing & Technology

T: +44 20 7809 2668

E: simon.bollans@shlegal.com

Darren Fodey

Partner

T: +44 20 7809 2388

M: +44 7920 201 290

E: darren.fodey@shlegal.com

STEPHENSON HARWOOD