Rail Cyber Security Strategy

Rail Delivery Group

National Rail

Contents

Navigate to section

Foreword

Alan Cain
CISO Rail Delivery Group

Modern life is characterised by the growing dependence of both individuals and businesses on digital technology. This encompasses a wide range of devices, including smartphones and tablets, as well as sophisticated digital applications in disciplines such as science and medicine. This rapid evolution has facilitated substantial progress, but it has also introduced substantial hazards, particularly in the form of cyber-attacks. Frequently orchestrated by individuals, organised groups, and even antagonistic nations, the UK Government has reported a consistent increase in these threats. The railway industry is one of the sectors that is at a higher risk.

The railway industry is particularly vulnerable to cyber threats due to its complex interdependencies and dependence on legacy software. In the event that critical systems are compromised, cyber incidents in this sector can result in reputational damage, operational disruptions, and, in severe cases, physical injury to individuals. In order to effectively address these challenges, it is imperative that the railway industry implement a robust cybersecurity strategy.

Despite ongoing endeavours to enhance cybersecurity throughout the railway network, there is a lack of consistency in protection levels and preparedness. The railway sector's industry-specific strategy emphasises the importance of collaborative measures to improve digital defences. This strategy identifies seven critical cybersecurity challenges and establishes five strategic objectives to enhance protection. It is accompanied by ten critical actions that are intended to achieve these objectives and reduce associated risks.

It is imperative to maintain ongoing efforts to enhance cybersecurity in order to reduce the financial and human costs of cyber incidents and to ensure compliance with the new EU and UK regulations that are designed to enhance digital security. The comprehensive strategy framework aids in the identification of anomalies, the protection of railway assets, the comprehension of cyber risks, and the effective response to mitigate the effects of cybersecurity incidents.

It is essential to capitalise on Britain's robust safety culture in order to foster a robust cybersecurity environment as the railway industry's digitisation advances. This method not only ensures the ongoing provision of safe, reliable, and efficient railway services but also establishes Britain's railway as a global leader in cybersecurity. The preservation of our railway's cyberspace must remain a top priority as digital threats continue to evolve.

Introduction

Great Britain's railway is an essential part of the country's national infrastructure, some of which is critical. Delivering safe, reliable and efficient railway services for passenger and freight users is a priority for the industry and government.

The increasing digitalisation and connectivity of train systems have significantly heightened cybersecurity risks to rolling stock. Key threats include ransomware and malware, which can encrypt critical data and disrupt train operations, as well as supply chain vulnerabilities that may introduce compromised components. Additionally, cyber-physical (CPS) attacks targeting control systems pose risks of operational disruption or even accidents. Other significant risks include interference with communication systems like GSM-R and Wi-Fi, sometimes resulting in erroneous signals or communication breakdowns; unsecured remote access points let attackers obtain illegal access. Advanced persistent threats (APTs) targeting critical infrastructure for long-term espionage or disruption significantly complicate the security scene by means of insider threats and weaknesses in third-party programs.

Reducing these risks requires rolling stock operators to apply a multi-layered cybersecurity plan. Strong access restrictions, regular vulnerability assessments, and network segmentation and monitoring help to stop and identify intrusions. Essential also are improving supply chain security, providing staff with comprehensive cybersecurity training, and developing robust incident response and recovery plans. By being proactive and using these technologies and methodologies, operators may better protect their systems, assure safety, and maintain the continuity of rail services while staying ahead of transforming cyber threats.

Rail Delivery Group

National Rail

Jacqueline Starr
Executive Chair & CEO, Rail Delivery Group

Our railways are more than just a way to travel; they connect people, communities, and businesses across the country every single day. As technology becomes increasingly central to how we operate and deliver services, protecting the railway from cyber threats has never been more important. We cannot afford to let digital risks undermine the safety, efficiency, and reliability of a system that so many people depend on.

This strategy is about much more than technical defences. It is about building a culture of awareness and responsibility across the entire sector, where every member of the railway community understands the part they play in keeping our systems safe. It is about working together as an industry, sharing knowledge, resources, and best practice, so that no organisation stands alone in the face of growing cyber challenges. And it is about planning for the future, making sure we are ready to face not only the threats of today but also those that are still to come.

With its clear objectives and practical actions, this strategy provides the roadmap we need to strengthen our resilience. By uniting rail operators, suppliers, government, and security experts, we can protect the railway from disruption and ensure it continues to deliver safe, reliable, and efficient services. Cyber security is a shared responsibility, and together we will keep our railway secure in the digital age and for generations to come.

WHAT IS THIS STRATEGY FOR?

This strategy ensures all stakeholders are informed, aligned, and empowered to contribute to the secure operation and evolution of the railway network.

PUBLIC / RAIL USERS

How the Strategy Helps Understand Cyber Security in the Railways

- Explains how cyber security measures ensure their safety and privacy when using rail services.
- Highlights protections methodologies for ticketing systems, personal data, and real-time passenger information.
- Builds trust by showcasing the commitment to resilience against cyber threats that could disrupt services.

MANAGING DIRECTORS

How the Strategy Helps Understand Cyber Security in the Railways

- Provides an overview of the business risks associated with cyber threats and their potential operational and reputational impacts.
- Offers actionable insights on how investing in cyber security supports business continuity and regulatory compliance.
- Demonstrates the financial and reputational benefits of a secure and reliable rail network.

RAILWAY COMMITTEES

How the Strategy Helps Understand Cyber Security in the Railways

- Clarifies their governance responsibilities in overseeing and ensuring a robust cyber security framework across the railway industry.
- Highlights the importance of collaboration and the need for collective action to manage systemic cyber risks.
- Aligns cyber security initiatives with broader industry goals such as digital transformation and passenger safety.

CYBER SECURITY PRACTITIONERS

How the Strategy Helps Understand Cyber Security in Railways

- Delivers detailed guidelines, technical frameworks, and best practices to mitigate specific cyber threats targeting rail systems.
- Supports practitioners in aligning their own organisational cyber security strategies with the overarching goals and frameworks of the rail industry.
- Promotes awareness of emerging threats, vulnerabilities, and incident response protocols tailored to the rail industry.
- Encourages collaboration and knowledge-sharing across the cyber security community to enhance resilience and innovation in rail systems security.

Strategic context

We live in an increasingly interconnected world with an ever-expanding threat landscape. The ability to deliver, innovate, and grow is heavily reliant on digital technologies, a vital enabler but also a potential vector for threats if not properly secured. Cyber security cannot be an afterthought, as the risks of failure could directly impact stakeholders and the public, as well as cause significant financial and reputational harm.

As our dependence on information systems and networks increases, so too do the opportunities for malicious actors to exploit vulnerabilities, whether through targeted attacks or as collateral damage from broader cyber activity. The growing threat from rogue nation states and cybercriminals underscores the need for robust and proactive measures.

This strategy emphasises the importance of embedding practices such as **Security by Design** and **Privacy by Default** into all projects and programmes across the rail industry. It provides a clear framework to ensure our approach to cyber security aligns with industry's best practices, delivering confidence to stakeholders safeguarding critical infrastructure from evolving threats.

Vision & Mission

Our vision is for the GB railway to provide a world-class service to its users by ensuring safety, protecting its cyberspace against hostile threats, and adopting interconnected technologies in an environmentally sustainable manner.

The Rail industry will be significantly hardened to cyber-attack by 2027.

The government national cyber strategy for the public sector is to be resilient to known vulnerabilities and attack methods no later than 2030, the rail industry aims to align with this timeframe.

Purpose of the Strategy

The purpose of this strategy is to provide a unified framework to protect the rail industry's critical infrastructure and digital systems against evolving cyber threats. It aims to safeguard the confidentiality, integrity, and availability of railway systems, ensuring the safety, reliability, and efficiency of services while aligning with legislative and regulatory requirements. By fostering collaboration, promoting a culture of cyber security awareness, and embedding robust security measures throughout the lifecycle of railway systems, the strategy supports innovation and the adoption of secure technologies. Through these efforts, the rail industry will enhance its ability to detect, protect against, and respond to cyber incidents, ensuring the resilience and security of the UK's rail network.

Department for Transport

RDG Cyber Strategy Preface

Our nation's railway infrastructure is a crucial part of our passenger and freight transport system that supports economic growth and is relied upon every day by businesses and individuals up and down the country. However, as the railway has become more interconnected and reliant on digital technologies, it has become significantly more vulnerable to cyber threats.

Securing our railway system requires more than just technical solutions. It demands a collective effort from all parties including passenger and freight rail operators, cybersecurity experts, government agencies and suppliers. By aligning our efforts, we can safeguard Britain's railways against cyber threats and build a future where our transport network remains a global leader in security.

This strategy sets out the complex cybersecurity challenges threatening the integrity and safety of our railways. With risks ranging from ransomware to advanced persistent threats targeting critical control systems, the stakes have never been higher. As cyber-attacks become more frequent and sophisticated, securing our digital infrastructure is essential.

This document outlines a unified approach to combat these evolving challenges. It sets a clear direction to strengthen our defences and highlights the importance of a culture of collaboration, awareness, and continuous improvement across the sector. Through five strategic objectives and ten critical actions, this will help our railway to remain safe, reliable, and resilient.

Crucially, cybersecurity must be seen as a foundational maintenance cost that delivers long-term benefits. Effective cybersecurity not only addresses immediate threats but also supports the resolution of operational issues, driving efficiency, cost savings and helping to achieve continuous service availability. This strategy reinforces the need for all stakeholders to treat cybersecurity as a baseline requirement, just as physical safety is non-negotiable, ensuring that it is never viewed as a competitive advantage, but as an essential, shared responsibility.

Let this strategy be the foundation for a secure, digitally resilient railway system that continues to serve society, safely and efficiently, for generations to come.

Benjamin Smith

Director, Public Transport Strategy and Security, Department for Transport

The challenge we face

The impact of cybercrime, cyber-attacks, and broader cyber incidents on the rail industry could be devastating, with long-term consequences for legacy systems and a potential loss of public confidence in rail services.

In today's world, we are all increasingly reliant on digital communications, which underpins much of our daily lives and business operations. This is particularly evident as the rail industry continues to evolve into a more digitally interconnected ecosystem. Cyber incidents pose varying levels of risk, from minor inconveniences to major disruptions. While not all risks can be eliminated, they can be effectively managed and mitigated through appropriate measures, robust systems, sound processes, and advanced technologies.

As a key provider of rail information and services, it is vital to adopt a consistent and systematic approach to information security across the organisation. By embedding principles such as Security by Design, Privacy by Default, and leveraging frameworks such as ISO/IEC 27001, The Data Protection Act (DPA), UK Government Cyber Security Strategy (2022–2030) ' we can ensure the resilience and security of our operations and maintain trust in the industry.

The challenge we face

Complex and Interconnected Systems

Modern railways are complex networks that integrate various subsystems, including signalling, ticketing, communication, and operational controls. The interconnectivity between these systems, while beneficial for efficiency, also increases the attack surface for potential cyber threats.

Legacy Systems Vulnerability

Many railway systems still rely on legacy technologies that were not designed with modern cybersecurity threats in mind. Upgrading these systems without causing disruptions to daily operations is a significant challenge.

Increasing Cyber Threat Landscape

The railway sector is becoming a more attractive target for cybercriminals and state-sponsored actors due to its critical role in national infrastructure. The threat landscape includes ransomware, data breaches, denial of service attacks, and espionage.

Real-Time Operational Risks

Railways require real-time data and control systems to operate efficiently. Cyber-attacks that disrupt these real-time operations can have immediate and potentially severe consequences for safety and service availability.

The challenge we face

Supply Chain Vulnerabilities

The railway industry’s reliance on a wide range of suppliers for software, hardware, and services introduces multiple points of potential vulnerability. Ensuring the cybersecurity of the supply chain is a complex but essential task.

Insider Threats

The human element remains one of the weakest links in cybersecurity. Insider threats, whether intentional or accidental, can lead to significant security breaches.

Regulatory and Compliance Challenges:

The railway industry is subject to stringent regulatory requirements related to safety and security. Ensuring compliance with these regulations while also addressing emerging cybersecurity threats requires ongoing effort and adaptation.

The challenge we face

Data Privacy Concerns:

Railways collect and store vast amounts of passenger data for ticketing, services, and operational efficiency. Protecting this data against breaches and ensuring privacy compliance is a critical challenge.

Skill Gap and Resource Constraints

There is a global shortage of skilled cybersecurity professionals. The railway sector competes with other industries for this limited talent pool, making it challenging to adequately staff cybersecurity teams.

Integration of New Technologies

The adoption of new technologies such as IoT devices, cloud computing, and AI in railway operations offers many benefits but also introduces new vulnerabilities and requires a revaluation of existing security protocols.

The challenge we face

Sophistication of Nation-State Attacks

Nation-state actors often possess sophisticated capabilities and resources, enabling them to conduct highly targeted and complex cyber-attacks. These actors may aim to disrupt railway operations for political, strategic, or economic reasons, posing a significant threat to national security and public safety.

Cybercriminal Profit Motives

Cybercriminals are primarily motivated by financial gain. They may target the railway sector with ransomware attacks, aiming to encrypt critical operational or customer data and demand ransom for its release. The reliance of railways on continuous operations makes the railway particularly vulnerable to such extortion attempts.

Emerging Threats and Advanced Technologies

As the railway sector incorporates more advanced technologies such as artificial intelligence, machine learning, digitisation of rolling stock and Internet of Things (IoT) devices, it also becomes exposed to new and emerging threats. These include AI-powered attacks that can learn and adapt to security measures, deepfakes that can manipulate personnel and operational data, and vulnerabilities in IoT devices that can be exploited to gain access to broader network systems.

Delivering the vision: objectives and actions

Achieving our cyber security vision is centred on five key objectives that guide the actions necessary to enhance the industry's security posture. These objectives define what we aim to accomplish across the rail sector as we work towards our mission and provide a clear framework for assessing and measuring progress.

The timeframe for delivery of the actions is between 2025 and 2030.

To support these objectives, ten targeted actions have been identified, reflecting our comprehensive approach to improving cyber security within the railway industry. These actions are designed to address varying levels of cyber security maturity and organisational priorities among stakeholders and are not ranked in order of importance. Instead, they offer flexibility to enable each organisation to tailor their focus based on their unique needs and circumstances.

Below we break down each objective and related actions that can be utilised to achieve compliance with the objective.

NCSC Director of National Resilience

“With millions of people relying on the rail network every day, protecting the critical systems and processes which underpin these services has never been more important – and we know cyber attackers are increasingly seeking to use our society’s technological dependence against us.

While stakeholders across the rail industry have together made significant progress in recent years raising the sector’s cyber resilience, it has not been at the pace necessary to match our adversaries. Opportunistic threat actors continue to present a persistent and potentially disruptive risk to the provision of essential services, including the UK rail network, and their suppliers.

It is therefore vital all operators from across the sector raise their security baseline, understand the cyber risks they need to manage, and prepare for how they would respond to an incident or a period of heightened risk.

Only through continued collaboration, information exchange and working together as a community to address the gaps in cyber security posture, can the UK effectively secure and ensure cyber resilience of rail infrastructure for the future.”

Jonathon Ellison
NCSC Director of National Resilience

OBJECTIVES

OBJECTIVE 1

Our people understand cyber security risk and act responsibly.

Securing our cyberspace relies on our people (everyone in our organisations and workforce who works with or for us) being aware of the cyber security risks, and the actions needed to protect our systems, and how to recognise and act on abnormal behaviour. Increased cyber security awareness and relevant skills leads to improved security behaviours and results in reduced exposure to threats.

We will develop a strong cyber security culture that is as effective as the industry's safety culture, which has zero tolerance for behaviour that could compromise passenger, workforce or public safety.

We will improve cyber security through driving changes in culture and human behaviour.

Security culture can be defined as the styles, approaches and values that the organisation wishes to adopt towards security.

For this strategy to be a success, everyone must understand the importance of cyber security in the railway and strive to ensure it is recognised.

Cyber security on the operational railway is in its infancy. In some other areas, such as safety and physical security, cultural change has been enforced through regulation. However, we can take a proactive approach to cyber security throughout our organisations.

Our people – our employees and contractors – will, through their actions, demonstrate commitment to protecting our organisations from cyber threats.

Why we should do this

A cyber security culture will provide us with people who understand the issues and can take ownership of cyber security, by:

- ✓ Encouraging the railway workforce to be Cyber Aware at home and work.
- ✓ Improving employee engagement to manage cyber security risk through understanding the potential impact of cyber incidents or attacks.
- ✓ Reducing risk of security breaches or incidents as employees think and act in a more security conscious way.
- ✓ Encouraging reporting of suspicious activities; reducing misuse of business information or systems; and improving incident response times.
- ✓ Increasing organisational effectiveness through adherence to policy.
- ✓ Improving internal and cross-industry communications on cyber security.
- ✓ Potentially, the way our employees behave can increase the risk of cyber-attack. Collectively improving the cyber security culture will provide our best defence.

Culture: Key activities

We will:

CULTURE

Understand the cyber security culture in our organisations and define the approach to improve it, ensuring we are aligned to our values.

ROLE MODELS

Create role models at all levels of the organisation to encourage good security behaviour by actively demonstrating awareness of, and commitment to, cyber security.

CREATING TRUST

Creating a culture based on trust where our organisations define the approach to cyber incident reporting and are encouraged to improve it. Ensuring we are aligned and employees feel empowered to challenge our values.

WORKING PRACTICES

Share good working practices and experiences. Organisations to encourage good security internally and with stakeholders. Develop behaviour by actively demonstrating ‘what good looks like’ and gain commitment to improved practice for the industry.

Culture: Key activities

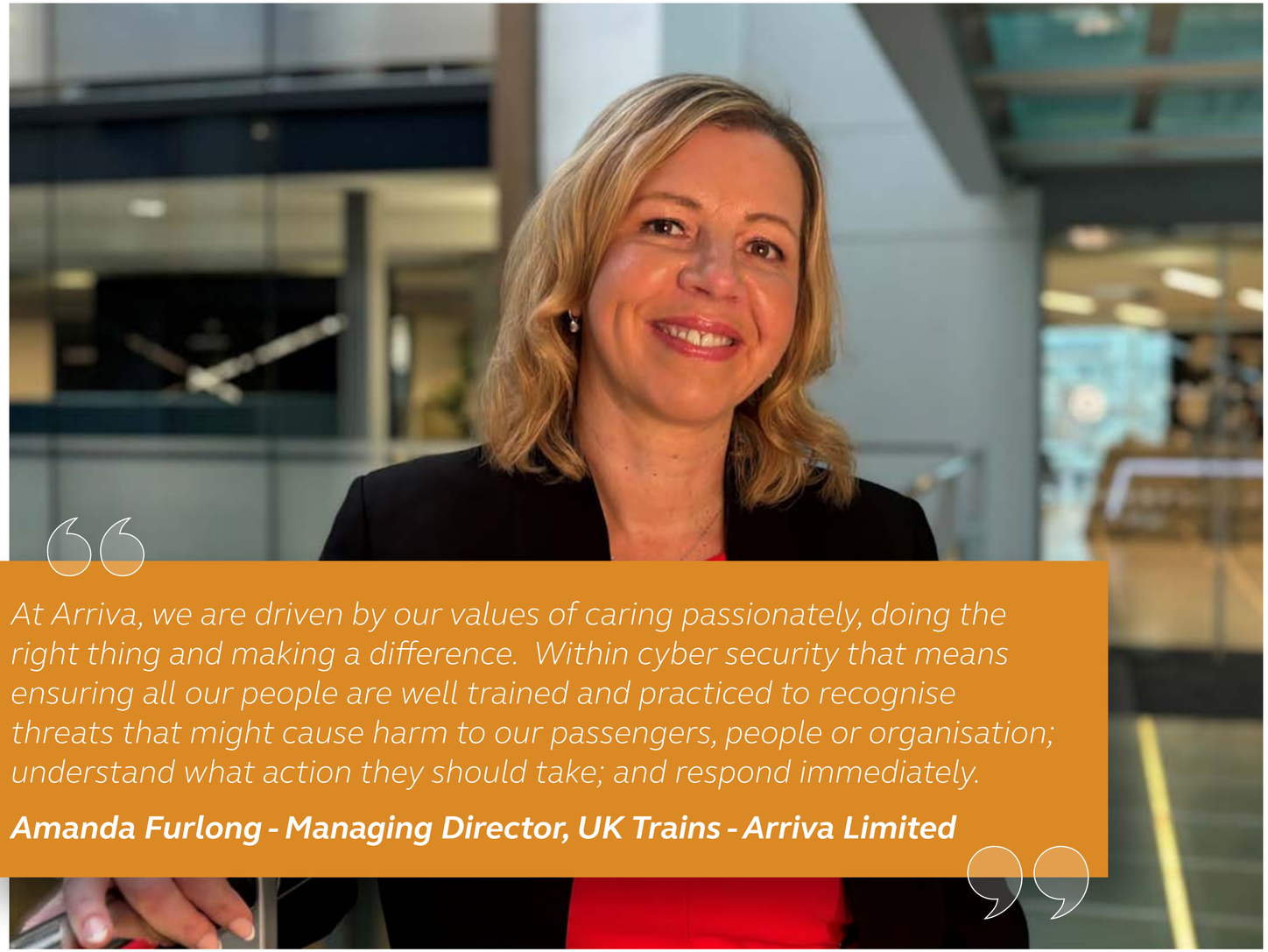
There will be a cumulative effect to improvements in cyber security across the railway cyberspace. To achieve our vision, railway stakeholders will be responsible for having an appropriate level of cyber security maturity across the railway that covers the identified action areas.

The following sections outline further detail on each action to deliver our objectives. Associated key activities have been identified for each railway stakeholder to progress across all technology environments, as appropriate, in their organisations, as part of the commitment to this strategy.

On-going training and relevant cyber security competency will provide the railway workforce with the knowledge needed to:

Make informed decisions to proportionately and appropriately manage cyber risk as appropriate for their role. Understand cyber security risks to the railway, our technology environments and business objectives, and how to identify events and respond appropriately. Protect the railway by minimising exposure to risk through the whole lifecycle of our systems. Understand where cyber security risk affects safety and reliability of the railway. Minimise the impact and duration of cyber security events by recognising, detecting, and reporting cyber security events, incidents, and suspicious behaviour.

Safety culture will be used as a model to achieve similar levels of commitment and determination to cyber security from our railway workforce.



At Arriva, we are driven by our values of caring passionately, doing the right thing and making a difference. Within cyber security that means ensuring all our people are well trained and practiced to recognise threats that might cause harm to our passengers, people or organisation; understand what action they should take; and respond immediately.

Amanda Furlong - Managing Director, UK Trains - Arriva Limited

We will develop an appropriate cyber security capability

We will ensure that people responsible for our business and operational systems know how to protect them appropriately.

Cyber security is evolving across the railway. Training our workforce will promote good cyber security, raise awareness of the threat posed by cyber-attacks, and ensure staff are able to make informed decisions.

Why we should do this

Competent, well-trained people play a crucial role in managing cyber security risk. Developing cyber security capability across all technology environments improves our ability to protect our cyberspace.

We will provide relevant, competency-based training and development experience that will keep pace with evolving threats to ensure our workforce can maintain an appropriate level of protection for our cyberspace.

Capabilities: Key activities

Training and competency development will develop cyber security capability in our organisations. Therefore, we will:

- Implement cyber security training programme(s) relevant to our organisations and individual roles, while recognising and complementing existing knowledge and skills.
- Produce a list of training and competency requirements for both our business and operational roles, and for those in our supply chain, at all lifecycle phases of our systems.
- Consider frameworks and industry apprenticeship schemes that provide experience, certification or professionalisation for roles with cyber security responsibilities.
- Assess ongoing cyber security competency of third-party suppliers. Implement a report and scoreboard to measure and improvement plan where required.
- Develop cyber security competent talent in house, and nurture and retain it, or employ new talent when necessary.
- Regularly share training initiatives and competency frameworks across organisations and the wider industry.
- Put into practice a competency management for safety, physical security and other working practices to be used as a model to manage cyber security training and competency for our workforce.

OBJECTIVE 2

We understand the extent and potential impact of our exposure to attack.

We can manage the exposure to attack of our cyber- space, the extent to which our systems are vulnerable to attack, and how widespread the impact is, as the threat to railway cannot be controlled. Understanding our exposure allows us to assess cyber security risk to provide appropriate protection for our cyberspace boundaries, legacy and modern digital systems, and railway interconnections.

We will take a risk-based approach to understand and manage the exposure of our cyberspace. By comprehensively assessing and mitigating potential vulnerabilities through a risk-based approach, we aim to strengthen our digital environment and ensure its resilience against evolving threats.

The railway has many interconnected digital technologies in different technological generations in a number of environments, which could be exposed to cyber threats.

The extent of our exposure depends on the complexity and accessibility of our systems, the ways in which they may be vulnerable, and the impact to our organisations of the loss or interruption of our railway services.

We must understand what systems and digital assets we have, where they are, what they do, who owns, operates and maintains them, how they are connected, their vulnerabilities, their lifecycle dependencies and the impact of their loss or failure.

Why we should do this

Identifying our digital assets is essential to secure cyberspace.

Knowing how our systems are connected and where we rely on each other, allows us to assess where our vulnerabilities are and how best to minimise the extent of their exposure, by:

- ✓ Identifying key systems or access points (interfaces) that need protection to minimise our potential attack surface.
- ✓ Identifying how information is stored and transferred and used by connected systems to understand how a cyber security incident may affect us and/or other stakeholders.
- ✓ Determining the operational importance, or criticality, of our systems as a prerequisite for carrying out a risk assessment.
- ✓ Identifying areas where we share common cyber security risk on the railway.
- ✓ Managing changes to ensure our cyber security related system information is accurate at all times.

Understanding Cyberspace: Key activities

We will build on existing knowledge of our systems to understand and manage how widespread an incident could be in the event of a cyber-attack.

DIGITAL ASSETS

We will produce a list that identifies our systems, digital assets (hardware and software components), locations, functions, owners, operators, support providers, third-party suppliers or other information to assess vulnerabilities and update information as systems change.

CYBERSPACE

Identify the scope of our cyberspace, security perimeters, security zones, conduits and interfaces that could be exposed to cyber threat. Record cyberspace interfaces where incidents could spread between organisations, systems, security zones, or functional areas.

DEPENDENCIES

Identify railway dependencies where impact could be greater in other organisations or systems.

PRODUCE A MAP

Produce a map of systems in our cyberspace to railway architectures based on accepted reference models to support consistent identification of boundaries, security layers and interfaces.

PROTECTION

Produce a prioritisation protection checklist of our systems, digital assets and interfaces based on the impact of the interruption or loss of their service(s), for example to our organisations or railway safety and reliability.

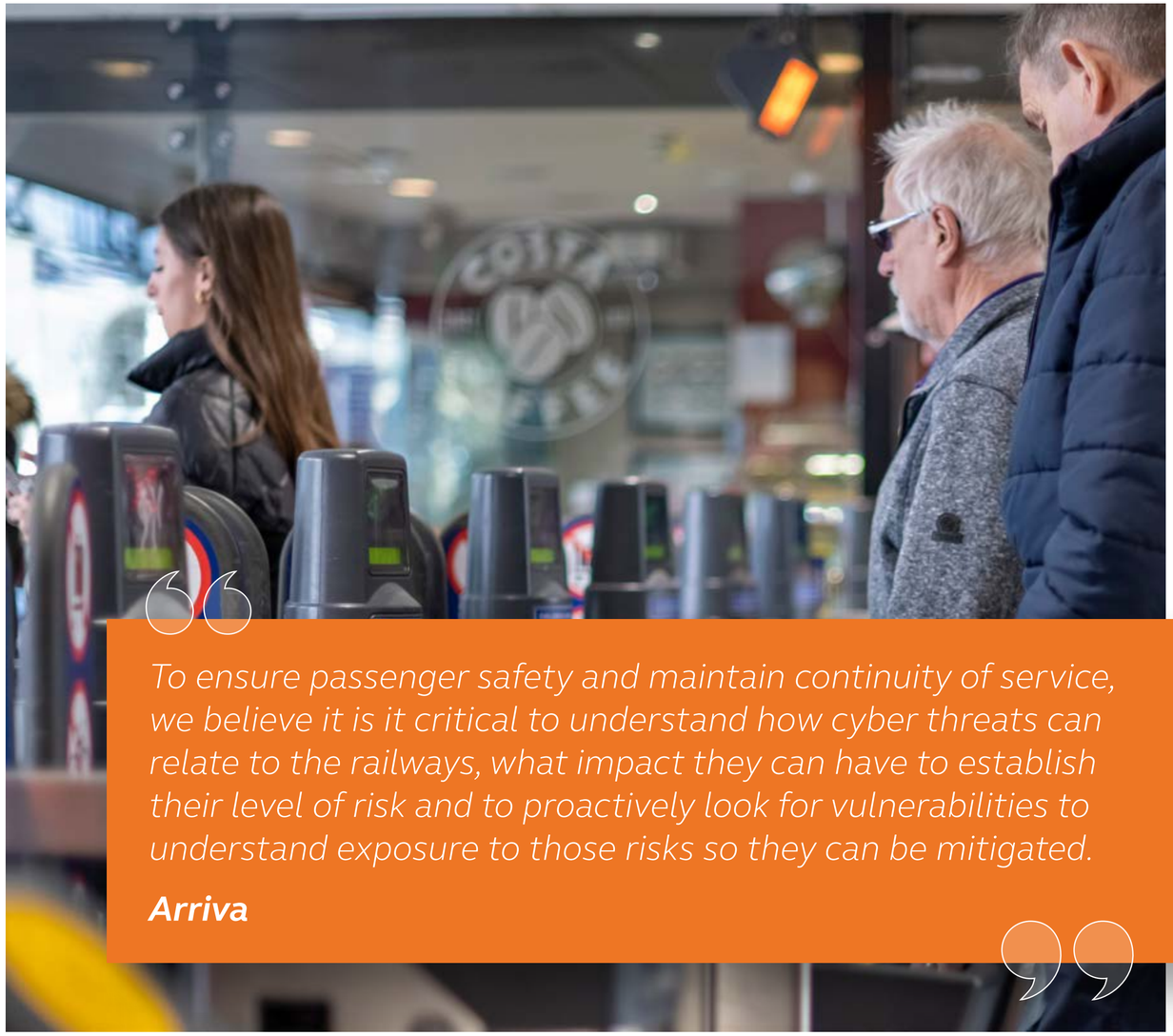
What we will do

- ✓ We will take a risk-based approach to understand and manage our cyberspace.
- ✓ We will adopt a risk-based approach to cyber security, so that our exposure is understood, and appropriate and proportionate security measures are taken to manage our cyber security risk.
- ✓ The implementation and management of our systems and processes will determine our exposure to attack. Risk management enables us to assess exposure and evaluate measures for keeping our systems secure.

Why we should do this

Risk management is a key part of effective cyber security. Legislation will require us to put in place cyber security risk management and assurance processes for our operational assets and communicate these to appropriate authorities.

Cyber security threats have the potential to impact the rail industry, affecting performance, safety and efficiencies. The introduction of security measures needs to balance the benefits of increased security and the capital and operational costs of these with any effects on employee roles, operation or system performance.



To ensure passenger safety and maintain continuity of service, we believe it is it critical to understand how cyber threats can relate to the railways, what impact they can have to establish their level of risk and to proactively look for vulnerabilities to understand exposure to those risks so they can be mitigated.

Arriva

Managing exposure: Key activities

To deliver a risk-based approach to cyber security, we will:

Implement robust and repeatable cyber security risk assessments for our systems based on threat modelling, vulnerability and impact assessment.

Set up an industry wide risk register to ensure cyber security has risk treatment and management plans in place to prioritise resources and actions.

Produce documentation detailing how to manage cyber security risk in an appropriate manner for systems where safety and/or reliability are important, as well as those where they may not be.

Set an agreed list cyber security risk levels for business and operational systems and their interfaces and manage these appropriately in our organisations.

Share information on cyber security risk management, which complies with legislation, supports development of common approaches across the industry and identifies common cyber security risks.

Put in place security measures which provide a defence-in-depth approach to manage prioritised cyber security risk. These include risk from people interacting with our systems (malicious intent or unintentional actions) and working practices that adhere to cyber security policies.

Taking a risk-based approach will allow us to:

EXPOSURE

Manage cyber security exposure through consistent and informed risk-based decision-making across our systems, organisations, and the wider industry.

RISK & EFFECTIVENESS

Consistently assess our cyber security risk and effectiveness of security measures.

REQUIREMENTS

Meet legislative requirements

ALLOCATE RESOURCES

Allocate resources effectively across our organisations based on risk prioritisation.

OBJECTIVE 3

Our defences operate consistently across our cyberspace, physical sites and organisations.

Reducing risk from threats requires a consistent approach across all systems, technology environments, functions, physical sites, and railway organisations because threats do not respect system or organisational boundaries. Consistent defences and risk management across the industry protects our cyberspace as its security is reliant on all of us.

We will have governance for cyber security in our organisations

We will provide executive-level support for cyber security across our organisations, with clearly defined governance structures and procedures.

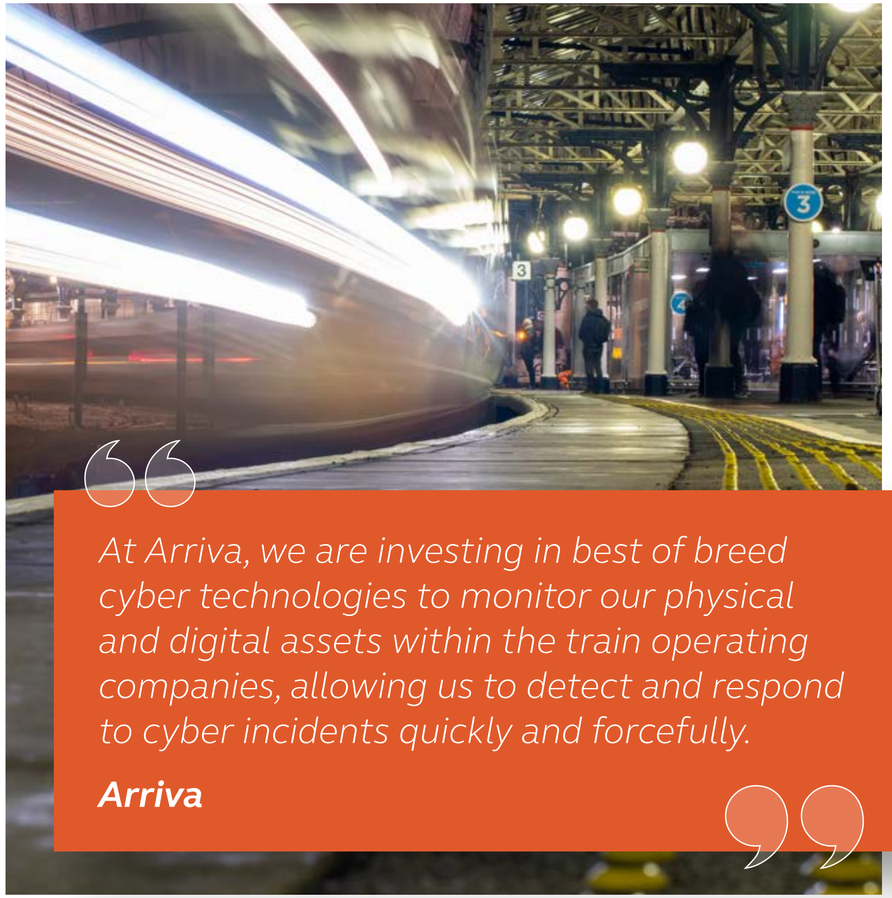
Governance for safety, physical security and other business areas, is already established in the rail industry. Cyber security governance provides a clear understanding for how the organisation will address its legal and fiscal responsibilities for cyber security.

Effective governance enables organisations to demonstrate commitment to cyber security, by:

- ✓ Delivering strategic direction (policy, standards, guidelines, and procedures) to manage cyber security consistently across the business.
- ✓ Allocating resources and funding to manage cyber security risk appropriately and proportionately.
- ✓ Taking a wider view of security measures across all technology environments and functional areas.
- ✓ Facilitating collaboration across the rail industry.
- ✓ Formulating and providing performance measurements for cyber security initiatives.
- ✓ Positively influencing the cyber security culture.

What we will do

- ✓ We will implement or develop cyber security governance in our organisations.



At Arriva, we are investing in best of breed cyber technologies to monitor our physical and digital assets within the train operating companies, allowing us to detect and respond to cyber incidents quickly and forcefully.

Arriva

Governance: Key activities

Successful and effective cyber security programmes require governance to be in place.
Therefore, we will:

ASSIGN & OWNERSHIP

Assign executive-level security risk ownership and allocation of cyber security roles, with clear and defined lines of authority, responsibility and accountability across all technology environments and functional areas.

CYBER SECURITY STRATEGY

Develop a cyber security strategy for our organisations that articulates and balances the needs of our business, its security objectives and the wider operational railway.

BUILD A BUSINESS CASE

Measure current cyber security against good practice and build a business case for a security programme and further initiatives as they are identified.

Governance: Key activities

Successful and effective cyber security programmes require governance to be in place. Therefore, we will:

RISKS & ALIGNMENTS

Collectively manage cyber security risk across the rail industry by collaborating with other railway organisations, ensuring strategic alignment to industry initiatives and regulation. Deliver a report detailing risks and relevant alignments.

SECURITY PERFORMANCE

Develop a consistent industry-wide security performance measurement system to support effective monitoring, control effectiveness and support continuous improvement, of our cyber security.

Activities may be incorporated into existing governance processes or structures to align with other strategic areas or organisational functions where effective and mutually beneficial.

We will ensure appropriate cyber security management of our systems and their interfaces

We will manage our systems and their technical and organisational interfaces consistently to reduce risk for the railway, and to increase our cyberspace resilience.

Railway cyberspace requires data exchange, such as traffic management and performance; customer information and train movement; timetabling, traction power management, station management and maintenance planning. System information is exchanged between stakeholders during the life of our systems.

Security defences at our perimeters and for our system interfaces protect the operational railway's technology, physical sites, and the railway stakeholders. Cyberspace threats span organisational and technology boundaries; therefore, we must also minimise the cyber security risk to everyone we interact with.

We will engage with domestic and international bodies on cyber security

We will work with relevant parties, including domestic and international bodies (for example EU institutions, agencies and academia), to influence policy, legislation, and guidance affecting the GB railway.

Collaboration will allow alignment of UK cyber security initiatives, ensure we learn from others, and provide an opportunity for others to learn from us.

We can influence opinion through representation and this will enable rail industry interests to be protected and our initiatives to be presented in a way that positions the GB railway at the forefront of cyber security.

Why we should do this

Working with a wide range of interested parties in relevant domestic, government and international bodies and other industry sectors will benefit the GB railway by:

- ✓ Ensuring domestic and international bodies take account of the GB railway's good practice, and cyber security strategy.
- ✓ Aligning policy and legislation with the approaches taken by the rail industry and recommended good practice.
- ✓ Ensuring the rail industry is informed of incoming legislation and policies.
- ✓ Learning about cyber security initiatives from other industry sectors.
- ✓ Influencing the DfT to incentivise investment in cyber security, for example by train operating franchisees.

What we will do

Engagement: Key activities

We will identify relevant parties and working groups with which to actively engage. We will share our cyber security vision and communicate this strategy, by:

- ✓ Promoting cyber security via delivery of a good practice guide detailing requirements within legislation, including Technical Specifications for Interoperability (TSI)18.
- ✓ Promoting inclusion of cyber security requirements, guidelines and good practice into domestic train operating franchise agreements via 'good best practice' guide.
- ✓ Support development of an assurance processes for cyber security to meet domestic and international legislative requirements.
- ✓ Encourage government investment and influence government decision-making about railway cyber security by producing a costed cyber security business case.
- ✓ Prepare a media plan to promote the GB railway as a leader in cyber security risk management.
- ✓ Share and exchange cyber security information with other industries, academia, councils, benchmarking groups, cyber-crime investigators, and other cyber security forums. Delivered through scheduled committee meetings, newsletters and bulletins.

OBJECTIVE 4

Our cyberspace is developed and managed to keep pace with evolving threats.

Securing our digital technologies is most effective when protection measures are designed and built in and when effectively maintained and improved during the whole life of our systems as new exposures or threats develop. Effective security intelligence, processes and lifecycle approach for systems allows us to deliver secure systems and keep up with the evolving threat.

We will work with third-party suppliers to manage cyber security in our supply chain.

We will work with our third-party suppliers to reduce the cyber security risk posed to the operational railway, to the largest extent possible.

The railway increasingly relies on third-party suppliers (vendors, contractors, service providers, and support organisations) to deliver products, systems, services, and resources to the operational railway.

Cyber security in the supply chain means that our procurement and assurance processes ensure these delivery partners design, build, supply, operate and maintain systems in a way that meets our expectations.

Our approach to addressing cyber security in our supply chain considers:

- ✓ The information we rely on (within or about our systems) as well as how and where information may be handled by our third-party suppliers, or their suppliers.
- ✓ The availability, not just of the information, but also of the third-party supplier and their products and services. For example, how we will access information or support our systems if our third- party suppliers are compromised or cease trading.
- ✓ The potential for the supply chain to be compromised, either as a result of different levels of cyber security or inadequate or inappropriate security measures.

Working with our supply chain allows us to:

- ✓ Reduce risk of cyber security events or incidents through the compromise of our trusted relationships or exposure through our supply chain, including loss of our information, for example drawings, designs, and software files.
- ✓ Understand the cyber security risks that a supply chain delivery may introduce at procurement and throughout the lifecycle, and how to appropriately manage them.
- ✓ Provide consistent and efficient cyber security risk management of our third-party suppliers and their delivery to the operational railway.
- ✓ Ensure all parties have the required security measures to monitor, detect, and respond to cyber security incidents

What we will do

We will work with our third-party suppliers and will encourage them to be secure businesses that deliver products and provide services to the railway that address cyber security risks.

Activities may be incorporated into existing supply chain or other business processes when these are effective and mutually beneficial.

Supply Chain: Key activities

To manage our exposure in our supply chain we will:

EMBED REQUIREMENTS

Embed cyber security requirements, or specify security measures, in procurement and support contracts with third-party suppliers. These will include cyber security for software development, as well as verification and validation measures for acceptance.

DELIVER A DASHBOARD

Deliver a dashboard that risk-assesses third-party suppliers, including business continuity and disaster recovery perspectives.

THIRD-PARTY COMETENCIES

Ensure third-party cyber security competencies and access to systems, including remote access, is in line with business requirements and managed from a cyber security perspective.

Supply Chain: Key activities

To manage our exposure in our supply chain we will:

CENTRALISED SYSTEM

Ensure third-party suppliers adhere to our cyber security policies or equivalent good practice for cyber security when working for us; use a centralised system to document certifications and compliance.

BENEFITS OF CONSISTENCY

Share good practices and align our requirements and assurance efforts to realise benefits of consistency in approach for the railway.

SUPPLY CHAIN INFORMATION

Share supply chain information, while complying with the law. We will also include cyber security requirements that allow us to share information on cyber security risk affecting our common systems or each other.

Why we should do this

Lifecycle cyber security risk management supports the resilience of the operational railway, by:

- ✓ Increasing threat intelligence to monitor and understand how threats are evolving.
- ✓ Reducing our exposure to, and the potential impact of, cyber-attack at the digital asset, system, interface, physical site, and organisational levels.
- ✓ Minimising interruption to services by managing system exposure through their life.
- ✓ Realising economic efficiencies of using secure-by-design principles, rather than retrofitting security, and assessing the efficacy of whole-of-life security measures.

We will ensure cyber security measures are applied through the life of our systems

We will build security measures into our systems and maintain and improve these to combat evolving cyber threats.

Taking a lifecycle approach needs us to specify cyber security requirements for our systems, ensuring these are procured, delivered and maintained during the life of the system, and that cyber security risk continues to be managed through decommissioning and disposal.

Cyber security risk to the operational railway can change for a variety of reasons. Managing our systems throughout their lifecycle will underpin the resilience of the operational railway.

Lifecycle: Key activities

To manage our exposure in our supply chain we will:

Actively monitor evolving cyber security threats and manage these accordingly.

Assign roles and responsibilities for the management of cyber security lifecycle activities.

Develop lifecycle cyber security approaches as early as possible including:

- Working with third-party suppliers to understand their products or services; define the lifecycles of our systems and digital assets and determine appropriate lifecycle cyber security management arrangements.
- Specification of cyber security requirements that incorporate secure-by-design principles into procurement and validate that third-party suppliers deliver them; for example, using technical security testing throughout its lifecycle.
- Delivery of appropriate and proportionate cyber security measures to reduce our exposure, manage our risk and minimise disruption or degradation of service through the life of our systems, as they are designed and built, operated and maintained, and when they become obsolete.
- Adhere to good practice design principles to deliver defence in depth to systems, using layers of security appropriate to the risk- based approach.
- Implement standards and guidance appropriate to the technology and environment to manage the cyber security of assets in a consistent way through their life.
- Operate and maintain security measures and, if necessary, improve these as new threats and exposures are discovered, with appropriate consideration for legacy assets as well as decommissioning or disposal of digital assets and technology.

OBJECTIVE 5

We are resilient to cyber incidents, can recover quickly, and learn from disruptions to improve.

Being able to recognise unauthorised or suspicious activity early improves our response to a cyber security event, which allows us to prevent an incident or minimise its potential impact. Monitoring our systems, sharing threat information and planning our response allows us to be prepared for cyber attacks resulting from the specific threat, the type of attack and systems affected in our cyberspace.

We recognise unauthorised activity and act swiftly to limit damage.

Having a cyber security incident response capability will enable us to minimise the effects of cyber security incidents by:

- Monitoring, detecting, and alerting on signs of compromise and cyber-related events, and implementing a reactive defence strategy.
- Possessing adequate threat intelligence to respond proportionately to cyber incidents.
- Initiating planned responses in a timely manner to:
  - Reduce the cost or other impacts on our organisation or stakeholders.
  - Minimise the time required for affected services to return to business as usual (delivering railway services).
  - Incorporate lessons learned from events or incidents to improve future plans.
- Meeting internal cyber security incident reporting requirements and complying with relevant legislation.

We will prepare for and manage cyber security incidents

Through collaboration, we will enhance our ability to prepare for, respond to, and report railway cyber security incidents.

Cyber security risk management reduces risk to an acceptable level, although some level of residual risk will remain. To build resilience of the operational railway, we need to enhance our understanding of the current cyber threat and be able to respond to cyber security events and incidents affecting digital assets.

Incident response policies and procedures will enable us to effectively recognise cyber security events and respond in a way that minimises the impact and limits damage when they become cyber security incidents.

The scale of a cyber security-related incident can vary, ranging from a short-lived localised occurrence on a single device or system, to a prolonged railway- wide occurrence affecting multiple systems and organisations.

Managing Incidents: Key activities

To prepare for cyber incidents we will:

SITUATIONAL AWARENESS

Develop our situational awareness by working collaboratively to understand our threat environment and the systems we need to protect. Implement proactive monitoring systems to detect abnormal behaviour, as appropriate.

WORK COLLECTIVELY

Work collectively and engage with third parties, other railway stakeholders and government organisations, through existing forums and groups, to improve threat intelligence.

ROLES & RESPONSIBILITIES

Define a list of specific roles and responsibilities for the management and implementation of cyber security incident response activities.

INFORM & CO-ORDINATE

Collectively inform and co-ordinate communications as an industry in response to major cyber security incidents. We will plan and document our external communications and delivery to the media and the general public in the event of a cyber security incident.

Managing Incidents: Key activities

To prepare for cyber incidents we will:

WORK COLLABORATIVELY

Work collaboratively to prepare and coordinate exercise of incident response plans based on realistic threat scenarios and lessons learned. We will align these with our other business resilience plans where appropriate, such as business continuity, disaster recovery, and internal and external communications plans.

APPROPRIATE CAPABILITIES

Develop appropriate capabilities in terms of people, competencies, processes, facilities and technology, to respond to cyber security incidents. This includes setting up a cyber security incident response team and the capability to collaborate with, provide sufficient evidence of incidents and report as appropriate to, external organisations, such as the DfT, BTP, Action Fraud and NCSC, to improve threat intelligence for the railway and other CNI.

REPORTING REQUIREMENTS

Consolidate cyber security reporting requirements and exchange information to improve efficiency for our organisations.

LONDON NORTH EASTERN RAILWAY

James Downey
LNER Finance Director

We are committed to strengthening cyber resilience through rigorous incident exercises, conducted both internally and with the support of key partners including British Transport Police (BTP), the City of London Police (CoLP), and the National Cyber Security Centre (NCSC). These exercises are crucial for preparing LNER to respond swiftly and effectively to potential disruptions, ensuring continuity even in the face of significant cyber incidents, such as a critical system compromise.

In parallel, our InfoSec team remains vigilant, actively monitoring a range of threat intelligence channels, including sources like RGD, NCSC, Interpol, and CISA. This continuous monitoring enables us to assess emerging threats and promptly identify risks specific to LNER and the broader rail industry. Following a Department for Transport (DfT) approved Cyber Security Information Sharing Strategy, we responsibly share pertinent information with affiliated Train Operating Companies (TOCs) and relevant organisations to reinforce the collective security of the rail sector.

A key part of our proactive approach involves robust email filtering systems designed to prevent spam and phishing attempts from reaching employee inboxes, serving as a first line of defence. In addition, we conduct both broad and targeted phishing simulations company-wide to sharpen our employees' cyber awareness. The Executive team is deeply committed to these initiatives, supporting the entire company's readiness to tackle phishing and other cyber threats.

Recognising the rail industry's reliance on select critical providers, we are also prioritising resilience planning to ensure that we remain operational in the event of a partner failure. Monthly threat intelligence reports are distributed to keep stakeholders informed about current and emerging risks, while all new employees undergo an induction programme highlighting the importance of identifying and reporting security risks. During Cyber Awareness Month, we run additional initiatives to reinforce security consciousness across the company.

Our communication strategy focuses on clear, accessible messaging that employees can relate to personally, underscoring how cyber vigilance safeguards both their professional and personal lives. We encourage the reporting of any security concerns, legitimate or otherwise, and position our workforce as the first line of defence.

In practice, these efforts include a brand protection application accessible to our Social Media Team, empowering them to flag scam accounts directly. Similarly, the "Report Phishing" button in Outlook allows employees to quickly report suspicious emails, which our InfoSec team actively manages. We have also implemented enhanced social media protections for VIPs, helping to prevent account takeovers and enabling swift alerts to our InfoSec team of any emerging threats. These combined efforts underscore our ongoing commitment to protecting LNER from cyber risks while fostering a culture of awareness and preparedness.

FUTURE THREATS IN RAIL CYBER SECURITY

As the cyber threat landscape continues to evolve, the rail industry must remain vigilant and adaptive to emerging risks. The strategy anticipates future challenges that could significantly impact the security and resilience of railway systems.

Quantum Computing and Cryptographic Risks

The advent of quantum computing poses a critical threat to the security of cryptographic systems that underpin modern digital infrastructure. Quantum computers could potentially break widely used encryption algorithms, rendering current methods of securing sensitive data and communications obsolete. This risk underscores the urgent need to explore quantum-resistant cryptographic techniques to protect rail systems against future vulnerabilities.

AI-Driven Cybercrime

Criminal actors increasingly leverage artificial intelligence (AI) to enhance their cybercrime capabilities. AI tools can be used to:

- ✓ Automate phishing campaigns with tailored, highly convincing messages.
- ✓ Exploit vulnerabilities faster and with greater precision through AI-driven reconnaissance.
- ✓ Evade detection using advanced malware capable of adapting to cyber defence measures.

The rail industry must integrate AI-driven defence mechanisms to counteract these threats and prevent the misuse of AI technologies against critical systems.

Nation-State-Sponsored Advanced Persistent Threats (APTs)

Nation-state-sponsored APTs remain a significant threat to critical national infrastructure, including railways. These sophisticated adversaries aim to disrupt operations, compromise sensitive data, and create widespread economic and societal impact. Their techniques often include:

- ✓ Persistent and covert infiltration of systems.
- ✓ Exploitation of supply chain vulnerabilities.
- ✓ Deployment of custom malware targeting industrial control systems (ICS).

To address this threat, the strategy emphasises collaboration with national cyber defence agencies, ongoing threat intelligence sharing, and strengthening the resilience of rail systems against prolonged and targeted attacks.

Proactive Measures for Emerging Threats

The strategy calls for proactive steps to mitigate these future threats:

- Regularly updating encryption methods to prepare for the quantum era.
- Investing in AI-powered defence tools to detect and respond to threats in real time.
- Enhancing monitoring and incident response capabilities to counter nation-state actors.
- Fostering international collaboration to share insights on emerging technologies and adversary tactics.

Increased Attack Surface Due to IoT Integration

The adoption of Internet of Things (IoT) devices across rail networks brings numerous advantages, including improved efficiency, real-time system monitoring, and predictive maintenance. However, these devices often have weaker security measures, creating vulnerabilities that can be exploited by adversaries. To address these risks, the following measures have been identified:

Secure Device Procurement and Deployment

- ✓ Ensure IoT devices meet recognised security standards and certifications.
- ✓ Conduct rigorous security assessments before deployment.

Network Segmentation

- ✓ Isolate IoT devices on segmented networks to minimise their access to critical systems.
- ✓ Deploy firewalls and intrusion detection systems to monitor and control traffic between IoT and other networks.

Regular Updates and Patching

- ✓ Maintain a schedule for applying firmware updates and security patches to IoT devices.
- ✓ Develop protocols to address vulnerabilities promptly.

Ongoing Monitoring and Threat Detection

- ✓ Use tools to monitor IoT devices for anomalous activities that may signal a breach.
- ✓ Integrate threat intelligence to proactively identify and mitigate emerging vulnerabilities.

By addressing these future threats, the strategy ensures that the rail industry remains resilient in the face of evolving cyber risks, safeguarding passengers, data, and operations.

RAIL SAFETY AND STANDARDS BOARD

Since publishing the first Rail Cyber Security Strategy, RSSB has strengthened its work to help the railway industry stay safe from cyber threats.

Listening to feedback, RSSB is creating a new strategy focusing on protecting the technology that keeps trains running. This approach helps organisations adopt modern digital systems with confidence while maintaining high standards of security. The goal is to use resources wisely and encourage collaboration across the sector.

To deliver this strategy, RSSB is working on three main priorities:

1. Reviewing the current state of cybersecurity in rail to understand where improvements are needed and how RSSB can help.
2. Publishing clear standards to guide the industry in building stronger defences.
3. Maintaining these improvements over time to keep the industry prepared for future challenges.

RSSB also represents Britain in developing international railway standards, including those covering cybersecurity. A team of experts ensures these standards are ready for use as soon as they are published.

As cyber threats continue to evolve, particularly for the systems that control train operations, RSSB will keep monitoring new risks and supporting the industry to stay protected.

Tom Lee
RSSB Director of standards

WHAT IS THE GOVERNMENT CYBER COORDINATION CENTRE (GCCC)

The Government Cyber Coordination Centre (GCCC) plays a critical role in the UK's cyber security landscape by enabling collaboration, intelligence sharing, and coordinated responses across public sector organisations. Aligning with the GCCC is essential for the rail industry as it provides access to real-time and actionable threat intelligence, allowing proactive mitigation of risks and improved situational awareness within the broader public sector context. Furthermore, the GCCC supports a unified and effective incident response, enabling rail operators to manage complex cyber incidents more efficiently through streamlined communication, resource allocation, and established protocols. By aligning with the GCCC, the rail industry can strengthen its defences, enhance resilience, and contribute to a collective security posture that protects critical national infrastructure.

Objective 1: People and Culture

‘Our people understand cyber security risk and act responsibly.’

Pillar 1:

Build Organisational Cyber Resilience

Action: Develop competency-based training and awareness programmes.

Action: Promote a zero-tolerance security culture similar to safety practices.

Pillar 2:

Defend as One

Action: Share training initiatives and frameworks across the rail sector and other public-sector bodies.

Specific Integration Actions:

Align workforce training with the UK Cyber Security Council’s standards.

Collaborate with the Government Cyber Coordination Centre (GCCC) to share best practices on incident reporting and cultural transformation.

Objective 2: Managing Exposure

‘We understand the extent and potential impact of our exposure to attack.’

Pillar 1:

Build Organisational Cyber Resilience

Action: Conduct comprehensive risk assessments for digital and physical assets.

Action: Maintain real-time asset inventories to monitor vulnerabilities and dependencies.

Pillar 2:

Defend as One

Action: Participate in shared vulnerability management and cross-sector information sharing.

Specific Integration Actions:

Use the Cyber Assessment Framework (CAF) to ensure consistent asset and risk visibility.

Adopt centralised tools for asset management and threat intelligence sharing across government entities.

Objective 3: Consistent Defences

‘Our defences operate consistently across our cyberspace, physical sites, and organisations.’

Pillar 1:

Build Organisational Cyber Resilience

Action: Implement defence-in-depth strategies using layered security controls.

Action: Standardise security configurations and governance across systems.

Pillar 2:

Defend as One

Action: Leverage government-wide protective measures for common threats.

Specific Integration Actions:

Standardise security controls and configurations across rail operations and align with government best practices.

Share frameworks for consistent defences across public-sector organisations.

Objective 4: Detection and Monitoring

‘We can identify, detect, and respond to cyber threats and incidents affecting railway operations.’

Pillar 1:

Build Organisational Cyber Resilience

Action: Develop internal monitoring and detection systems for early threat identification.

Pillar 2:

Defend as One

Action: Collaborate with the GCCC to enhance cross-sector situational awareness.

Specific Integration Actions:

Establish centralised security operations that integrate rail detection systems with government-wide threat intelligence platforms.

Enhance the use of automated detection tools to scale incident identification.

Objective 5: Resilience and Recovery

‘We are resilient to cyber incidents, can recover quickly, and learn from disruptions to improve.’

Pillar 1:

Build Organisational Cyber Resilience

Action: Conduct regular incident response exercises and update recovery plans.

Action: Build resilience by integrating security into system lifecycles.

Pillar 2:

Defend as One

Action: Share lessons learned from incidents with government and industry partners.

Specific Integration Actions:

Use government-led recovery frameworks and templates to ensure rapid restoration of services.

Participate in cross-sector incident response exercises for improved readiness.

Rail Delivery Group

National Rail