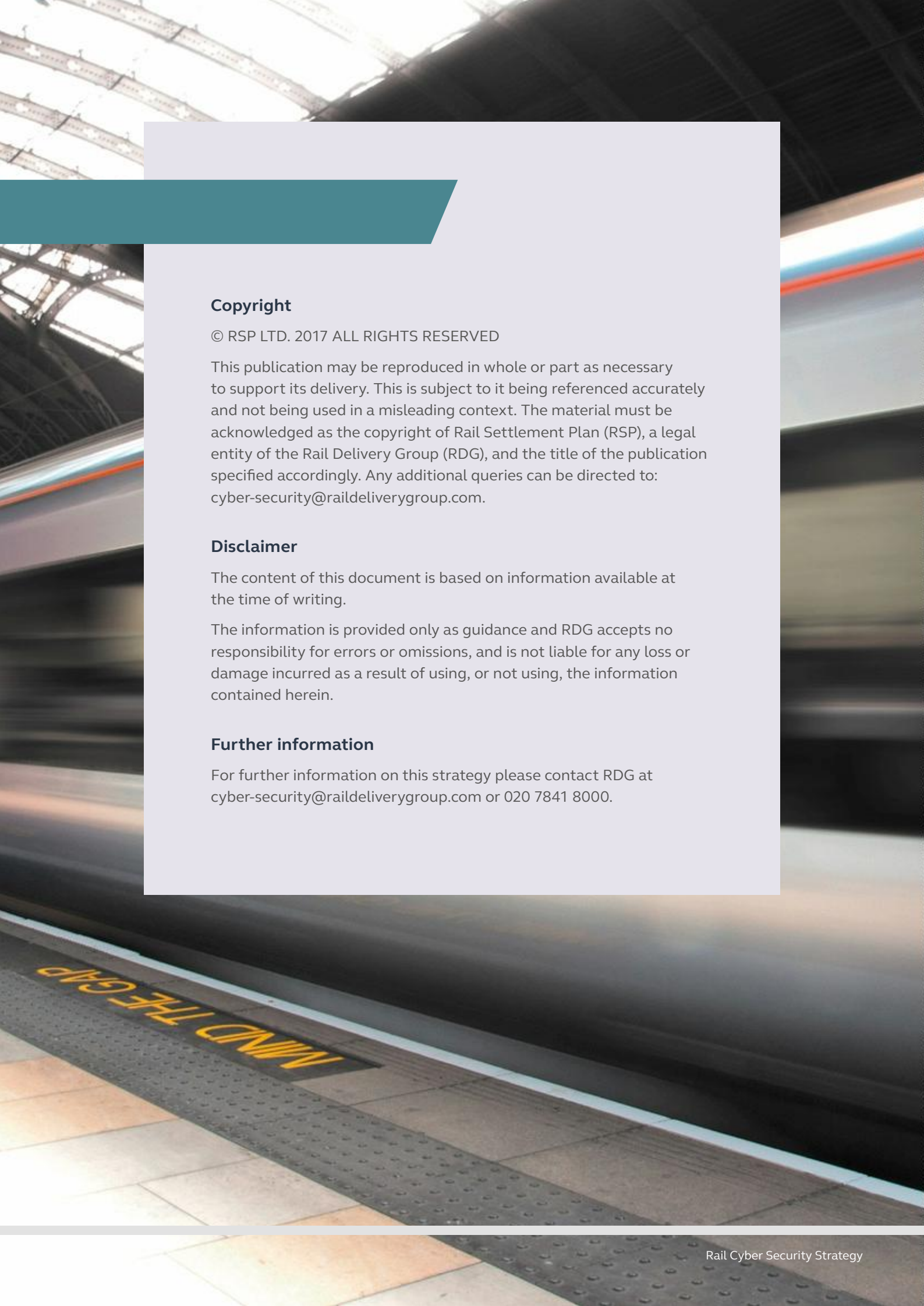
Rail Delivery Group

National Rail

BRITAIN RUNS ON RAIL

Rail Cyber Security Strategy

January 2017 | Release 1.1



Disclaimer

The content of this document is based on information available at the time of writing.

The information is provided only as guidance and RDG accepts no responsibility for errors or omissions, and is not liable for any loss or damage incurred as a result of using, or not using, the information contained herein.

Further information

For further information on this strategy please contact RDG at cyber-security@raildeliverygroup.com or 020 7841 8000.

FOREWORD

Businesses and individuals are increasingly dependent on digital technology. From the ubiquitous smartphones and tablets that many of us rely on to run our lives, through to the most advanced use of digitised technology in science and medicine, the digital revolution is influencing daily life.

This step change, which is gathering pace at an extraordinary rate, has resulted in huge advances. But the widespread use of digital communications also carries a significant risk in the form of cyber attack, from individuals, organisations and hostile countries. Indeed, the UK Government indicates the threat from cyber attack is rising steadily.

The railway, of course, is not immune to the threat of cyber attacks; cyber incidents have already affected the industry and, as this strategy clearly shows, there is potential for future attacks that could result in a range of possible outcomes, from reputational damage through to disruption and even injury and loss of life due to systems being compromised.

Embracing the need for robust cyber security and being prepared for cyber attacks represent significant challenges for our industry, with its complex interdependences and legacy infrastructure. Some important measures have already been taken, but currently there are different levels of preparedness and protection across the various parts of the railway.

This strategy, which has been developed by the railway for the railway, sets out in detail how railway stakeholders that deliver Britain's railway services will work together to protect our cyberspace. It highlights: seven cyber security challenges that are specific but not unique to the railway; five cyber security objectives that will enable the delivery of our vision for cyber security; and, crucially, ten actions that will be required to achieve the objectives and overcome the challenges.

Continued action to address cyber security risk to the railway will enable the industry to reduce the impact, both financial and human, of cyber security attacks and incidents, and prepare for incoming legislation. New European Union (EU) and UK legislation is aimed at protecting Britain's railway from cyber attack; the rail industry must respond quickly and positively to reduce its impact.

This strategy is the framework for our response. It will help us to: understand cyber risk and the impact of cyber incidents; protect railway assets by safeguarding the confidentiality, integrity and availability of digitised technology; detect abnormal behaviour in people, assets or systems; and respond in a way that reduces the impact of cyber security incidents on safety, services, and people.

Britain's railway has established safety mechanisms in place, and is widely recognised as one of the safest railways in Europe. Britain's rail industry now has an opportunity to use its enviable safety record as a model for creating a culture of cyber security in the industry that can lead the way and be widely recognised as good practice.

It is essential that we continue to deliver safe, reliable, and efficient railway services as we face ever evolving cyber threats. As the inevitable digitisation of the railway progresses we must act together, now, to protect our railway cyberspace.

ACKNOWLEDGEMENTS

This strategy has been created with the help of the industry's Cyber Security Advisory Group (CSAG), made up of cyber security experts from the following organisations.

RDG thanks these organisations for their contribution:

- Abellio
- Arriva
- Rail Delivery Group (RDG)
- British Transport Police (BTP)
- National Cyber Security Centre (the successor to the Centre for the Protection of National Infrastructure (CPNI))
- Institute for Security Science and Technology at Imperial College London
- Colas Rail
- Crossrail
- Department for Transport (DfT)
- GB Railfreight
- Great Western Railway
- The Go-Ahead Group
- London Midland
- Network Rail
- Office of Rail and Road (ORR)
- PA Consulting Group
- Porterbrook
- RSSB
- Stagecoach

We also acknowledge the below organisations for their contribution to the development of the strategy:

- Adelard
- Angel Trains
- Eversholt Rail Group
- Freightliner Group
- London Overground Rail Operatins Limited (LOROL)
- Private Wagons Federation
- RazorSecure
- Resonate
- Railway Industry Association (RIA)
- Siemens
- Transport for London (TfL)
- Thales

CONTENTS

INTRODUCTION

Great Britain's railway is an essential part of the country's national infrastructure, some of which is critical.[1] Delivering safe, reliable and efficient railway services for passenger and freight users is a priority for the industry and government.

Digital technology is already widely deployed on the railway. Modern computer-based business and operational systems are used to improve reliability, efficiency, capacity and the customer experience of the rail network. Several high-profile projects, such as Crossrail, HS2 and the Thameslink modernisation programme, rely on such systems to meet their objectives. These developments, however, mean the railway could become a potential target for cyber attack, resulting in one or more of the following impacts for railway stakeholders that deliver railway services:

- Threat to safety of the workforce, passengers or the public resulting in harm.
- Disruption to railway services.
- Financial loss, including to the wider UK economy.
- Loss of commercial or sensitive information.
- Criminal damage.
- Reputational damage.
- Failure to comply with law.

To protect against the wider threat of cyber attacks, the UK Government and the European Union (EU) are developing new legislation. Complying with this will ensure the rail industry is better prepared for cyber threats.

In advance of the introduction of this new legislation, the Department for Transport (DfT) and the Centre for the Protection of National Infrastructure (CPNI) asked RSSB to facilitate development of a cross-industry cyber security strategy for the rail industry.

In working together to produce this strategy, railway stakeholders have agreed a shared vision to improve protection from, and resilience to, evolving cyber threats:

Our vision

Our vision is that the GB railway delivers a world-class service for its users, by protecting its cyberspace from hostile threats as it continues to embrace interconnected digital technologies.

This strategy supports the vision and the Rail Technical Strategy objective that all information systems must be resilient to cyber attacks (RTS, 2012), while not limiting innovation in the railway. The strategy was handed to RDG in December 2016 for its onward development, including guidance, support and monitoring of its delivery.

1: As defined by the UK Government (http://www.cpni.gov.uk/about/cni/)
2: NCSC have taken over CPNI's responsibilities on cyber security.

1.1 Who should read this document

This strategy is primarily aimed at rail industry leaders (particularly those who are responsible for cyber security); and senior managers in railway stakeholder organisations. The strategy will also be a valuable point of reference for government organisations, the Office of Rail and Road (ORR), the Rail Supply Group (RSG), and the Railway Industry Association (RIA) and its members.

This strategy focusses on the operational systems that provide railway services and their supporting business systems, including those providing passenger services. Other business or enterprise systems are not excluded. Railway stakeholders that are responsible for the security and resilience of GB's operational railway services (set out in Table 1 on page 11) are responsible for the implementation of this strategy.

1.2 Railway digital technology

Technology is critical to the railway, supporting business and operational needs. Broadly, computer-based railway systems can be divided into two environments that have varying cyber security risks, business drivers and potential impacts of loss or failure:

1. **Business systems** deliver corporate or enterprise functions, and also include systems that support and provide interface to the operational railway such as rostering, time-tabling, passenger services and information, telecommunications, ticketing and revenue. The roles of people providing cyber security in this environment include: operational security teams, information technology (IT) and human resources (HR) staff, data protection officers, facilities, finance, procurement teams and managers.
2. **Operational systems** enable the operational railway to function through control of network infrastructure and rolling stock, such things as train movements, signalling, power, telecommunications, and station management. These systems may be referred to as operational technology (OT). The roles of people providing cyber security in this environment generally include: operational cyber security teams, design engineers, maintenance engineers, operators of railway digital technology, safety engineers and managers.

Technology is enhancing efficiency and customer service across the railway. This means that the two environments are converging so that:

- Information is increasingly exchanged between business systems, operational systems and organisations to support railway performance and safe interworking.
- The industry is increasingly reliant on computer-based technology, now common to both environments, which has security implications.

Organisational and system interfaces, as well as the workforce using the technology, also increase the exposure of the railway. Additionally, a large and widely dispersed volume of railway assets, which can be difficult to protect, could provide access points for cyber threats.

1.3 Our approach to cyber security

The railway's increasing reliance on interconnected digital[2] technologies, increases its exposure to cyber attack. This is also affected by dependencies between organisations and systems to deliver railway services.

The UK Government recognises cyber attack as a Tier One risk to UK interests, and we welcome the fact that the transport sector is included in the revised UK Cyber Security Strategy (HM Government, 2016). Effective cyber security will reduce the risk of cyber security incidents and will help maintain GB railway's position as one of the safest in Europe (ORR, 2015).

We, as railway stakeholders, are responsible for the security and resilience of the operational railway. We have individual business and commercial drivers and varying levels of cyber security maturity and appetite for risk.

To improve cyber security across the whole railway we must collaborate with each other, and with the DfT, British Transport Police (BTP), ORR, UK National Cyber Security Centre (NCSC), and other government organisations involved in the protection of UK critical national infrastructure (CNI).

As our cyberspace is only as strong as the weakest link, we are taking a whole system view of the railway.

Our proactive approach to cyber security is based on three principles to provide a clear and consistent direction for the industry. These are shown in Figure 1.

Figure 1 Description of cyber security elements key to the strategy

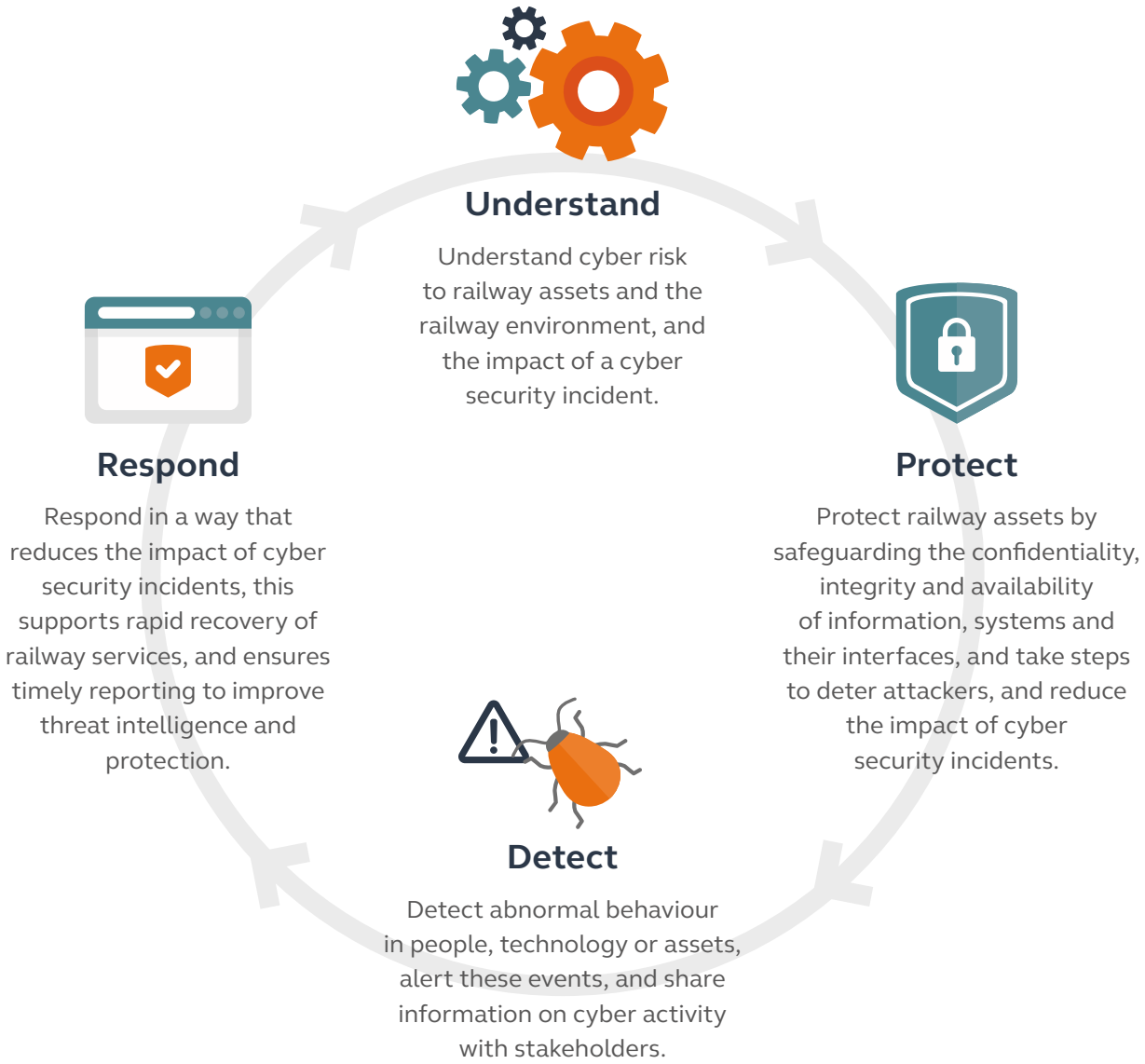
Build on what exists	Take responsibility	Work collaboratively
Our actions will align with common cyber security frameworks, recognised good practice, and our existing organisation structure and processes.	We will commit to addressing cyber security within our organisations and take an appropriate and proportionate approach to manage our cyber security risk.	We will work together to share information to improve protection against cyber threats to the railway.

2: Cyber and digital are synonymous in this document.

To achieve a consistent approach across a diverse railway, we will use this strategy as the basis for developing our own organisational plans for cyber security.

We will look within our organisations and look out to the wider industry in each of the core elements of cyber security. Figure 2 shows the cyber security elements that form the basis of the strategic approach.

Figure 2 Description of the rail industry's key strategy principles



1.4 Working together to strengthen railway cyber security

Minimising the risk from cyber attack will require close collaboration by the rail industry; we all have a role in protecting the railway.

Figure 3 shows the high-level relationships to maintain and deliver cyber security for the GB railway.

We must work together, as a cyber attack affecting one system or organisation may spread to cause much wider impact.

Table 1 on the following pages sets out the roles of the organisations that will ensure cyber security for the GB railway.

Figure 3 Working together to strengthen cyber security

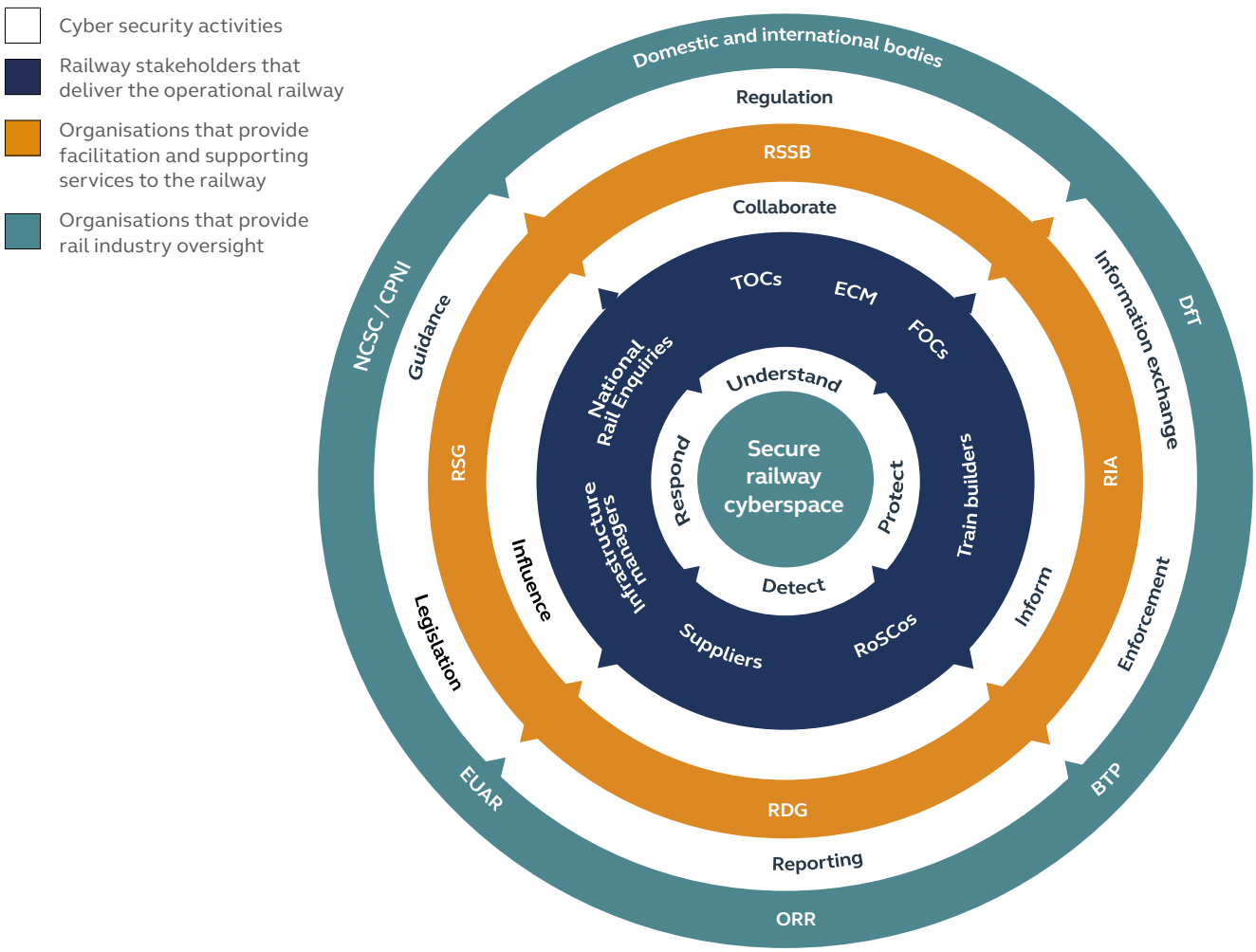


Table 1 Securing railway cyberspace: the key players and their roles

	Institution or organisation	Role in delivering rail cyber security
Railway stakeholders that deliver the operational railway	Those that collectively deliver the GB railway services: • Train Operating Companies (TOCs) • Freight Operating Companies (FOCs) • Infrastructure Managers (IMs) • National Rail Enquires • Suppliers • Rolling Stock Owning Companies (RoSCo) • Train Manufacturers (builders) • Entities in Charge of Maintenance (ECM)	Procure and supply products and services with consideration for cyber security. Ensure systems delivering railway services have appropriate and proportionate cyber security risk management through their lifecycle. Company executives are responsible for cyber security risk and ensuring it is managed in their part(s) of the railway.
Industry partners that provide facilitation supporting services	• Rail Delivery Group (RDG) • Railway Supply Group (RSG) • Railway Industry Association (RIA) and its members • RSSB (http://www.rssb.co.uk)	Provide facilitation services and support to enable infrastructure managers, train operating companies and freight operating companies to work together.
Organisations that provide rail industry oversight	Department for Transport (DfT) https://www.gov.uk/government/organisations/department-for-transport	Legislates on security, including cyber security.
	British Transport Police (BTP) http://www.btp.police.uk/	Provides law enforcement. Cyber incidents, where terrorist or criminal activity is suspected might be reported to the BTP.
	Rail sector of National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/	Provides a unified source of advice and support on cyber security for UK industry including the management of cyber security incidents and CNI. Provide guidance and tools for industry, as well as threat intelligence and alerts, for example the Cyber Security Information Sharing Partnership (CISP).

	Institution or organisation	Role in delivering rail cyber security
Organisations that provide rail industry oversight	Office of Rail and Road (ORR) http://orr.gov.uk/	Safety regulator with an interest in cyber security risk.
		Cyber incidents that impact safety might be reported to the ORR.
	European Union Agency for Railways (EUAR) http://www.era.europa.eu/Pages/Home.aspx	Supports delivery of safe, modern, and integrated railway networks, including support on technical matters for EU interoperability and ERTMS.
		Develops requirements for EU railways and manufacturers in the form of Technical Specifications for Interoperability (TSI) and supporting documents that might contain cyber security.

1.5 Understanding cyber security risk

According to the UK government, the threat from cyber attacks is increasing; cyber incidents have already affected railways.

The risk from cyber attack is a product of: vulnerability, or susceptibility to harm; threat, or intent to cause harm; and likelihood. Determining risk requires an assessment for each of these.

The likelihood of an individual or organisation to launch a successful cyber attack depends on: motivation, capability (skills, knowledge and information) and access.

We need to identify the threat sources, threat actors and threat types that may affect our cyberspace.

People from inside or outside an organisation can be a threat source (those who wish to compromise systems) or threat actors (those who actually carry out an attack)[4].

Potential threats

Potential threat sources and actors include: terrorists, criminals, foreign intelligence services, competitors, hackers, activists, malware developers, employees, and contractors.

We need to protect our cyberspace from accidental as well as intentional cyber security threats, which may lead to cyber attacks that exploit vulnerabilities in people, processes or technology and impact our railway services (as previously set out). A representation that cyber security activities provide defence for our systems against potential impacts from the cyber security threats above is shown in Figure 4.

4: There may be cases where a source may influence, coerce, or mislead an actor to launch an attack on their behalf.

Figure 4 Cyber security activities manage risk to the railway

Cyber attacks can be for financial gain; political or commercial interest; or personal satisfaction.

The nature and severity of an attack will depend on the intent, resources, and technical capability of the threat source or actor. The likelihood of an intentional cyber attack on the railway is influenced by the attractiveness of our cyberspace, our exposure, and the current threat landscape. The threat intelligence we have affects our ability to be prepared for cyber attack, while limiting opportunity and having security measures in place manages cyber security risk and provides levels of defence to our systems.

1.6 Protecting railway cyberspace

Railway cyberspace comprises the digital systems (assets and their networks) that underpin both business and operational systems, including all information and data[5] stored in and transferred through these networks. This includes systems that deliver operational railway functions such as signalling, power, rolling stock, communications, track, stations and customer information to support effective business decisions such as remote support, maintenance, condition monitoring and system optimisation. The cyber security landscape for the operational railway is illustrated on the reverse page of this document.

5: Data and information are synonymous in this document.

The railway is continuing to increase digitisation to bring improvements for users, which increases cyber security risk.

The DfT has identified that vulnerabilities exist in the rail industry as cyber security provision is variable (DfT, 2016). Therefore systems may be susceptible to deliberate and non-deliberate cyber attack, and need to be appropriately protected.

Cyber security is delivered through a set of technical, procedural and managerial security measures[6] to ensure that confidentiality, integrity and availability are not compromised. A cyber attack may adversely affect a railway system's availability, reliability or ability to fulfil its required function.

Railway cyber security is the protection of our cyberspace and is complemented by both physical and personnel security measures. Although these are not the primary focus of this strategy it must be recognised that there are strong dependencies and that cyber security provides an input to overarching railway security.

6: Measures and controls are synonymous in this document.

2. ACHIEVING OUR VISION

As an industry we will work together to achieve our shared ambition for securing our evolving railway cyberspace: our vision is shown in Figure 7. We will do this by overcoming the cyber security challenges we face and prepare for cyber security legislation that will affect the railway, whilst sharing a common mission.

Our mission

Our mission is to ensure our current and future railway technologies are appropriately and proportionately protected from the risk of cyber attack, by taking a collaborative, unified, and lifecycle approach to efficiently deliver cyber security.

To support our mission, that outlines what we will do and why, we have identified key steps to deliver our vision, shown in Figure 5 below.

2.1 Delivering the vision: objectives and actions

Delivering our cyber security vision depends on five objectives that drive the cyber security actions that we will deliver, and provides a means to assess and measure our progress in achieving our vision. These objectives outline what we will accomplish across the railway as we progress towards the mission.

Ten actions have been identified to deliver the objectives, based on our approach to improving cyber security in the railway (see Section 1.3). The actions are not prioritised as the cyber security maturity and organisational focus will be different for each railway stakeholder.

Figure 6 summarises the objectives and the key actions. Details of each action and the key activities are in Section 3.

Figure 5 Key steps to deliver our cyber security vision for the railway

Defined a set of principles and common approach for cyber security to provide a clear and consistent direction for the industry.

Set ourselves specific objectives that define the targets we, as railway stakeholders, must reach to achieve our vision.

Identified the key actions that we, as railway stakeholders, will take to meet our objectives.

Figure 6 Summary of objectives to achieving our vision and the key actions to deliver them

Our vision

Our vision is that the GB railway delivers world class service for its users by protecting its cyberspace from hostile threats as it continues to embrace interconnected digital technologies.

Our Mission

Our mission is to have our current and future railway technologies appropriately and proportionately protected from cyber attacks, through a collaborative and united approach to cyber security.

Objective 1	Objective 2	Objective 3	Objective 4	Objective 5
Our people understand cyber security risk and act responsibly.	We understand the extent and potential impact of our exposure to attack.	Our defences operate consistently across our cyberspace, physical sites and organisations.	Our cyberspace is developed and managed to keep pace with evolving threats.	We recognise unauthorised activity and act swiftly to limit damage.
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 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.	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.	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.	Being able to recognise unauthorised or suspicious activity early improves our response to a cyber security event, which allows us to prevent and 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.
Actions				
1. We will develop our cyber security culture. 2. We will develop an appropriate cyber security capability.	3. We will understand our cyberspace. 4. We will take a risk based approach to understand and manage the exposure of our cyberspace.	5. We will have governance for cyber security in our organisations. 6. We will ensure appropriate cyber security management of our systems and their interfaces. 7. We will engage with domestic and international bodies on rail cyber security.	8. We will work with third-party suppliers to manage cyber security in our supply chain. 9. We will ensure cyber security measures are applied through the life of our systems.	10. We will prepare for and manage cyber security incidents. Sharing knowledge across the industry and working closely with the NCSC.

2.2 Railway cyber security challenges

The rail industry faces cyber security challenges, like other areas of CNI. The GB railway also faces specific issues because of its operating environment, legacy infrastructure, and the application of new digital technology.

Table 2 sets out a high-level summary of those considered most significant by the industry[7] and shows which actions work to overcome them.

Table 2 Challenges facing the rail industry

Challenge	Summary of the challenge facing the railway	Overcome by Action
Managing the cyber security risk due to increased connectivity of business and operational systems	Our cyberspace is exposed due to increasing connectivity between business and operational systems. This is compounded by the vulnerability of legacy systems; slow adoption of cyber security in engineering practices; and the high number of geographically dispersed assets. The workforces that deal with business and operational systems also have different skills and levels of experience.	1, 2, 3, 4, 5, 6, 8, 9, 10
Managing cyber security risk for system interfaces	Interconnectivity increases interfaces and, consequently, our attack surface. This exists at all levels, from lineside equipment through to business systems. Currently, our cyberspace is not sufficiently understood to enable appropriate management of our systems and their interfaces.	3, 4, 5, 6, 9, 10
Managing cyber security of the supply chain	Our supply chain is complex, interdependent, sometimes international and evolving. This, together with a reliance on third-party suppliers has led to more information exchange about our systems and consequently an increased cyber security risk. The lack of common cyber security requirements has also resulted in different levels of cyber security in products and services across the railway.	1, 3, 4, 5, 6, 7, 8, 9, 10
Managing safety risk and cyber security risk	Developing an integrated safety and cyber security culture is challenging because of sometimes conflicting priorities and processes between the two. Commonalities and differences need to be appropriately managed.	1, 2, 5, 8, 9, 10
Cyber security collaboration	There are different levels of preparedness and protection across the railway. Increasing awareness of how, what and why information should be shared for the good of the whole operational railway may encourage collaboration and information exchange on cyber security initiatives.	4, 6, 8, 9, 10

7: Sources include Cyber Security and Resilience of Intelligent Public Transport (ENISA, 2016), CSAG industry knowledge and experience and DfT Rail Cyber Security – Guidance for Industry (DfT, 2016)

Challenge	Summary of the challenge facing the railway	Overcome by Action
Acquiring cyber security funding	Showing why cyber security is a priority and securing funding for cyber security initiatives , and ongoing operational expenditure for security monitoring and response capability is an on-going challenge. The structure of the railway, with train operating franchises providing relatively small windows for investment, poses an additional funding challenge.	5, 7
Collaboration with domestic and EU bodies	Interoperability, safety regulations and other EU directives impact on the railway. Having the right level of representation and an influence on decision-making will achieve the best outcomes.	7

2.3 Preparing for incoming cyber security legislation

Changes to UK and EU cyber security legislation are extending to the rail industry, which means railway stakeholders will be required to be aware of and comply with new laws, let alone the standards and good practices of ISO27001/2, the General Data Protection Regulation (GDPR) and Cyber Essentials Plus. The aim of this strategy is to prepare the industry to effectively mitigate cyber security threats to our railway cyberspace; in doing so we recognise that effective cyber security measures and implementation of this strategy will support meeting incoming legal obligations (as known at the time of release), which are summarised in the following sections.

2.3.1 Directive on security of network and information systems

The Directive on security of network and information systems (NIS Directive) is a EU Directive which aims to ensure a high level of cyber security in the EU by mandating improved national cyber security capabilities and co-operation between member states and sectors.

The NIS Directive came into force in August 2016 and member states were given 21 months to transpose the NIS Directive into their national laws; it will apply from May 2018.

Railway infrastructure managers and railway undertakings are identified in the NIS Directive under the types of entities that could be 'operators of essential services' within transport (European Commission, 2016). If UK railway stakeholders are designated as 'operators of essential services' they will be required to:

- Implement risk management practices, to 'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations'.
- Report significant cyber security incidents to a 'competent national NIS authority' and / or the national 'Computer Security Incident Response Team' for the UK this will be the NCSC. The competent authority will be responsible for the application of the Directive for the sector.

8: The UK Computer Emergency Response Team (CERT-UK)

2.3.2 DfT measures under the Railways Act 1993

The DfT has responsibility for setting and enforcing railway security standards for the GB railway, with operators responsible for the delivery of security and bearing the cost. The DfT actively works with the rail industry, BTP and wider government partners, to ensure that risks are understood and that mitigation measures are targeted, proportionate and practicable. Security regulations (instructions), along with good practice guidance, are issued on behalf of the Secretary of State to train operating companies, Network Rail and others with an involvement in all facets of railway security. In February 2016, the DfT issued guidance, Rail Cyber Security (DfT, 2016), to support the rail industry in reducing its vulnerability to cyber attack.

Under Section 119 of the Railways Act 1993, the Secretary of State can issue security instructions to railway operators to ensure that measures are taken to prevent acts of violence to persons and property, including terrorism, resulting from cyber threats. The DfT has been working with industry and other partners to ensure that appropriate and proportionate measures, including regulation, will be put in place for the heavy rail sector from 2017 to protect the railway's critical operational systems from cyber attack. This includes proposed requirements for risk assessment, response planning, incident reporting and the identification of suitable points of contact.

2.3.3. General Data Protection Regulation (GDPR)

The Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is a new EU Regulation and Directive which aims to reform data protection rules across the EU, to unify data protection and ease the flow of personal data across the member states.

The General Data Protection Regulation (GDPR) came into force in May 2016 and member states were given 24 months until the GDPR becomes law in their countries, and also to transpose the Directive (focused on policing) into their national law; both will apply from May 2018.

Every organisation that processes EU residents' personally identifiable information (PII) will be required to abide by the provisions of the new law or face significant penalties. (European Commission, 2016) In the UK it supersedes the UK Data Protection Act (1998), and has a broader definition of personal data.

Railway stakeholders that store employee or user PII, or process their data, will be required to be aware of, and comply with, their new obligations, including: obtaining consent; mandatory privacy risk assessments; notification of data breaches; privacy by design; and discarding data. GDPR could apply to competency management, and will have more effect on the business systems, such as HR, ticketing, billing, and user or customer information.

3. ACTIONS TO IMPROVE SECURITY ACROSS THE RAILWAY

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 (see Section 2.1). 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.

3.1 We will develop our cyber security culture

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' (CPNI, 2014).

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.

3.1.1. Why we should do this

Potentially, the way our employees behave can increase the risk of cyber attack[9]. Collectively improving the cyber security culture will provide our best defence.

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**[10] 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.

9: As shown by research, such as that undertaken by the CERT® Insider Threat Centre at Carnegie Mellon University (www.cert.org/insider-threat/)
10: HM government initiative, formerly Cyber Streetwise, for increasing cyber security awareness (https://www.cyberaware.gov.uk)

3.1.2 What we will do

We will develop a strong cyber security culture that is as effective as the industry's safety culture,[11] which has zero tolerance for behaviour that could compromise passenger, workforce or public safety.

Culture: Key activities

Increasing cyber security awareness will develop a strong cyber security culture in our organisations. Therefore we will:

1. Understand the cyber security culture in our organisations and define the approach to improve it, ensuring we are aligned to our values.
2. Create role models at all levels of the organisation to encourage good security behaviour by actively demonstrating awareness of, and commitment to, cyber security.
3. Create a culture based on trust where cyber incident reporting is encouraged and employees feel empowered to challenge others.
4. Share good working practices and experience, internally and with other stakeholders, to establish 'what good looks like' and good practice for the industry.

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

3.2 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.

3.2.1 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.

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.

11: Safety culture is 'the way we do things around here', in other words how well employees and managers work together to tackle safety issues: RSSB Safety Culture Information (http://www.safetyculturetoolkit.rssb.co.uk/safety-culture-information/what-is-safety-culture.aspx)

3.2.2 What we will do

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:

1. Develop cyber security training programme(s) relevant to our organisations and individual roles, while recognising and complementing existing knowledge and skills.
2. Address different training and competency requirements for both our business andoperational roles, and for those in our supply chain, at all lifecycle phases of our systems.
3. Consider frameworks and industry apprenticeship schemes that provide experience, certification or professionalisation for roles with cyber security responsibilities.[12]
4. Assess ongoing cyber security competency of third-party suppliers.
5. Develop cyber security competent talent in house, and nurture and retain it, or employ new talent when necessary.
6. Share training initiatives and competency frameworks across organisations and the wider industry.

Competency management for safety, physical security and other working practices could be used as a model to manage cyber security training and competency for our workforce.

3.3 We will understand our cyberspace

We will identify our systems and their interconnectivity to understand how and where they could be affected by cyber attacks or incidents.

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.

12: As part of the National Cyber Security Programme, various government departments have worked with professional bodies and academia to develop a comprehensive cyber security competency framework for specialists. The resulting framework is published by the IISP (https://www.iisp.org/imis15) and sets out the competencies for cyber security professionals.

3.3.1. Why we should do this

Identifying our digital assets is essential to secure our 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.

3.3.2. What we will do

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. We will:

1. Identify 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.
2. Identify the scope of our cyberspace, security perimeters, security zones, conduits and interfaces that could be exposed to cyber threat.
3. Identify cyberspace interfaces where incidents could spread between organisations, systems, security zones, or functional areas.
4. Identify railway dependencies where impact could be greater in other organisations or systems.
5. Map systems in our cyberspace to railway architectures based on accepted reference models[13] to support consistent identification of boundaries, security layers and interfaces.
6. Prioritise protection 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.

13: DfT Rail Cyber Security – Guidance to Industry' (DfT, 2016) provides information on an architecture reference model relevant to the railway.

3.4 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.

3.4.1 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.

Understanding the risks and the potential for losses or failure to achieve legal obligations supports delivery of security measures that are right for our railway and represent efficient control of risk.

We cannot protect every digital asset to the same degree. A risk-based approach allows us to make optimum use of resources to protect our assets in a manner proportionate to their exposure or impact.

Taking a risk-based approach will allow us to:

- **Manage cyber security exposure** through consistent and informed risk-based decision-making across our systems, organisations, and the wider industry.
- **Consistently assess our cyber security risk** and effectiveness of security measures.
- **Meet legislative requirements** (See Section 2.3).
- **Allocate resources effectively** across our organisations based on risk prioritisation.

3.4.2 What we will do

We will have a consistent approach to assessing cyber security risk. We will use established methods for assessing safety risk as a model to achieve similar levels of consistency for cyber security.

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

Managing exposure: Key activities

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

1. Put in place robust and repeatable cyber security risk assessments for our systems based on threat modelling, vulnerability and impact assessment.
2. Ensure cyber security risk is held on an appropriate risk register and has risk treatment and management plans in place to prioritise resources and actions.
3. 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.
4. Agree cyber security risk levels for business and operational systems and their interfaces, and manage these appropriately in our organisations.
5. 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.
6. 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[14]), and working practices that adhere to cyber security policies.

14: The Holistic Management of Employee Risk (HoMER) guidance from CPNI provides a useful resource (http://www.cpni.gov.uk/advice/personnel-security1/homer/)

3.5 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.

Formal cyber security governance will ensure ownership of the cyber security risk, define our cyber security risk management approach, and allow informed decisions to be made.

3.5.1 Why we should do this

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.

3.5.2 What we will do

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

Governance: Key activities

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

1. Ensure assignment of 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.
2. 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.
3. Measure current cyber security against good practice and build a business case for a security programme and further initiatives as they are identified [15].
4. Collectively manage cyber security risk across the rail industry by collaborating with other railway organisations, ensuring strategic alignment to industry initiatives and regulation.
5. 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.

15: The CPNI ICS Security Assessment Tool provides a mechanism to assess the extent to which an organisations is achieving good practice as outlined in the CPNI SICS Framework. https://www.ncsc.gov.uk/guidance/security-industrial-control-systems

3.6 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.

Interfaces are where systems, people, or organisations meet and exchange information. Railway cyberspace has two types:

1. Technical interfaces that exchange data between digital assets or security zones.
2. Organisational interfaces where information is transferred via electronic or physical media.

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.

3.6.1 Why we should do this

Managing the cyber security risk of our systems and their interfaces improves our security posture, allowing us to:

- **Intelligently defend or protect** staff, passengers, assets, systems, physical sites and organisations and minimise our attack surface.
- **Provide security measures** to minimise the spread of cyber security incidents, and potential impact on other stakeholders.
- **Safeguard systems** by controlling access and sharing of information about them.
- **Provide a consistent and proportionate level of protection** across our cyberspace.
- **Comply with the law**.

3.6.2 What we will do

We will use existing safety risk procedures, such as the duty of co-operation,[16] as a model for cross-industry co-operation on cyber security for our interfaces.

Cyber security risk levels and maturity vary across the railway; therefore similar security measures might not be applied on both sides of an interface.

Managing Interfaces: Key activities

Consistently managing the cyber security risk of our systems and their interfaces is key to effective cyber security. Therefore, we will:

1. Work collaboratively to define the level of criticality of our interfaces by assessing both sides of the interface for dependencies and impact, and manage cyber security risk (See Section 3.4).
2. Assign roles and responsibilities for the management of interfaces within and between organisations.
3. Ensure information exchange across our interfaces is identified, classified, and managed in accordance with security policies.
4. Deliver cyber security measures to protect our information, and restrict or limit information exchange to only those digital assets, physical sites, systems, and people necessary to provide the services or functions needed.
5. Share information of cyber security risk at interfaces (system dependencies, impact, or threat information) with those on the other side and identify shared cyber security risk, and/or cyber security incident response plans.
6. Support the development of common approaches to security-informed safety cases, cyber security risk assessment, and adoption of internationally accepted standards across the industry.

16: As mandated by Regulation 22 of Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) (as amended) http://orr.gov.uk/__data/assets/pdf_file/0020/2567/rogs-guidance.pdf

3.7 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[17] 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.

3.7.1 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.

3.7.2 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, to:

1. Promote cyber security good practice and requirements within legislation, including Technical Specifications for Interoperability (TSI)[18].
2. Promote inclusion of cyber security requirements, guidelines and good practice into domestic train operating franchise agreements.
3. Support development of assurance processes for cyber security to meet domestic and international legislative requirements.
4. Encourage government investment and influence government decision-making about railway cyber security.
5. Engage with the media to promote the GB railway as a leader in cyber security risk management.
6. Share and exchange cyber security information with other industries, academia, councils, benchmarking groups, cyber crime investigators, and other cyber security forums.

17: An example of a group that can be influenced via the DfT is the EU 'Expert Group on Land Transport Security (E02821)' (http://ec.europa. eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2821)
18: Technical Specifications for Interoperability (http://www.era.europa.eu/Core-Activities/Interoperability/Pages/TechnicalSpecifications.aspx)

3.8 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.

3.8.1 Why we should do this

Proactive management of our supply chain, including financial, technical, and contractual elements, will provide us with third-party suppliers who are managing cyber security risk and working with us to protect our systems.

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.

3.8.2 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:

1. 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.
2. Risk-assess third-party suppliers, including from business continuity and disaster recovery perspectives.
3. 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.
4. Ensure third-party suppliers adhere to our cyber security policies or equivalent good practice for cyber security when working for us.
5. Share good practices and align our requirements and assurance efforts to realise benefits of consistency in approach for the railway.[19]
6. 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.

19: The CREST Cyber Essentials scheme provides a HM Government assessment framework for orgnaisations, whereby they can certify they meet specific information security controls (http://www.cyberessentials.org/index.html)

3.9 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.

3.9.1 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.

3.9.2 What we will do

Lifecycle: Key activities

To manage our exposure in our supply chain we will:

1. Actively monitor evolving cyber security threats and manage these accordingly.
2. Assign roles and responsibilities for the management of cyber security lifecycle activities.
3. 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 assests, 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.
   - Ensure standards and guidance appropriate to the technology and environment are in place to manage the cyber security of assets in a consistent way through their life.
4. 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.

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

3.10 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.

3.10.1 Why we should do this

Having a cyber security incident response capability will allow us to minimise the effects of cyber security incidents, by being able to:

- **Monitor, detect, and alert signs of compromise** and cyber related events, and implement a reactive defence strategy.
- **Have adequate threat intelligence** to respond proportionately to cyber incidents.
- **Initiate planned responses** in a timely manner, which:
  - Reduce the cost or other impact to our organisation or other stakeholders.
  - Minimise the time in which affected services are able to return to business as usual (delivering railway services).
  - Include learning from events or incidents for improvement of plans.
- **Meet internal cyber security incident reporting requirements** and those included in legislation.

3.10.2 What we will do

Responding to cyber security incidents is a key part of effective cyber security and we will actively work together as an industry to prepare for these.

Managing Incidents: Key activities

To prepare for cyber incidents we will:

1. Develop our situational awareness by working collaboratively to understand our threat environment and the systems we need to protect. Proactively monitor our systems to detect abnormal behaviour, as appropriate.
2. Work collectively and engage with third parties, other railway stakeholders and government organisations, through existing forums and groups, to improve threat intelligence.
3. Define specific roles and responsibilities for the management and implementation of cyber security incident response activities.
4. Collectively inform and co-ordinate communications as an industry in response to major cyber security incidents. We will plan our external communications and delivery to the media and the general public in the event of a cyber security incident.
5. 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.
6. Develop appropriate capabilities in terms of people, competencies, processes, facilities and technology, to respond to cyber security incidents.[20] This includes cyber security incident response teams 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.
7. Consolidate cyber security reporting requirements and information exchange to improve efficiency for our organisations.

20: NCSC SICS Framework and the CPNI First Responders Guide both provide information in this area.

4 ASSESSING THE IMPACT OF THE STRATEGY

This strategy will need to be regularly reviewed to assess its impact for the rail industry, in terms of adoption and realisation of benefits.

4.1 Governance

The responsibility for working together to deliver this strategy lies with the railway stakeholders that are responsible for the implementation of this strategy (see Table 1).

We envisage that railway stakeholders and other rail industry leaders will confirm their commitment to the shared cyber security vision and industry-wide objectives, and actively support initiatives to deliver the key actions for improving cyber security, both within their organisations and the wider industry.

The Head of Cyber and Technology, on behalf RDG's Technical Services Director, will be the custodian of the 'Rail Cyber Security Strategy'. The RDG Board will be accountable for the governance of the strategy, whilst the Technical Services team will ensure processes are put in place to monitor, review and update it on at least an annual basis.

RDG will work with stakeholders, not least the CSAG, DfT and NCSC, to determine whether the strategy is being addressed, and will seek to guide, support and coordinate its delivery. Where appropriate, offering a central core function to address common threats and vulnerabilities whilst resolving interconnection/ boundary issues.

4.2 Railway stakeholder maturity assessment

A secure railway cyberspace depends on the cumulative effect of cyber security improvements. Railway stakeholders will need to consistently self-report on the maturity level for cyber security to support overall monitoring of the strategy.

It is recommended that the rail industry adopt a consistent approach to assess the cyber security maturity of railway stakeholders.[21]

For example, railway stakeholders at a high level of cyber security maturity would be able to demonstrate, for both business and operational systems, where an interruption of service could lead to a potential impact on the operational railway. At a high level of maturity, stakeholders will be able to demonstrate that:

- Cyber security governance structures and procedures are in place.
- Cyber security training and awareness programmes are established and competency frameworks are in place.
- Asset registers or inventories cover all relevant systems.
- System boundaries, interfaces and dependencies are identified.
- Cyber security risk assessments are completed and proportionate risk management is in place, for all relevant systems. Boundaries, interfaces, and dependencies are included, as appropriate.
- Third-party suppliers are identified and cyber security risks assessed and managed as appropriate.
- Cyber security requirements have been established for the lifecycle phases for all relevant systems, and risk management plans put in place.
- Incident response plans are in place for all relevant systems.

21: CPNI, National Institute of Standards and Technology (NIST) and US Department of Homeland Security (DHS) have developed tools to support industries with this task, for example CPNI ICS Security Assessment Tool, NIST Common Security Framework and DHS Cyber Capability Maturity Model.

4.3 Monitoring

Impartial monitoring of the impact of the strategy is essential to its success, and RDG will work collaboratively with the industry to establish these arrangements. These will be substantially based on self-assessment, as well as feedback and self-reporting by collaborative groups.

We anticipate that these will be in the following areas:

- Progress of delivering implementation plans for this strategy.
- Overall evaluation of railway stakeholder maturity assessment (see Section 4.2).
- Degree of adherence to consistent cyber security risk management approach.
- Level of participation in industry-wide threat intelligence or incident response planning.
- Level of participation in industry-wide training initiatives or alignment to competency frameworks.
- Degree of alignment to industry-wide boundary identification, interface risk assessment, or reference architectures.
- Evaluation that appropriate collaboration has been undertaken to evaluate cyber security risk for interfaces in railway cyberspace.
- Evaluation that relevant industry bodies are identified, and appropriate industry-wide collaboration plans are established.

RDG are working with stakeholders to develop an automated Cyber Security Self Assessments Tool in an attempt to simplify, standardise and accelerate the near-term identification and prioritisation of local, group and national level risks in order that these may be coordinated and addressed at the appropriate level.

4.4 Review

Annual review of progress on delivery of the different areas of the strategy. The review of the strategy is recommended, taking into account:

- Cyber security arrangements in the rail industry.
- UK and EU cyber security legislation.
- UK government threat intelligence.
- Industry adoption of international standards and good practice, for example those listed in the Further Reading section.

5 SUMMARY OF ACTIONS

Action is needed to achieve our cyber security vision in recognition of the railway as a key part of the UK CNI.

This strategy provides the framework for our success, so that we are effectively mitigating cyber security risk; prepared for the legislation that will affect the rail industry; leading the way in cyber security for CNI; and delivering our own cyber security objectives.

Accepting the roles we have and the risks we share, we will work together to protect ourselves and each other from the ongoing threat of cyber attack.

For all of our interconnected digital technologies across the business and operational environments of the modern railway we will take appropriate and proportionate steps towards a secure railway cyberspace.

Ten actions have been agreed to ensure cyber risk is understood, our systems are protected, cyber security events are detected, and we can respond effectively. These are to:

1. Develop our cyber security culture

We need to increase cyber security awareness to: encourage good cyber security behaviours in our people; ensure the workforce understand their responsibilities and take ownership of cyber security risk, as appropriate; and encourage good security practice across the railway.

2. Develop an appropriate cyber security capability

We need to train our people to ensure that people using our systems understand security threats, their individual responsibilities to protect our systems and what action they should take in response to a cyber security event or incident.

3. Understand our cyberspace

We need to know our cyberspace to understand our exposure and the potential impact of cyber attacks, by identifying our: information systems (the railway's digital assets and their networks), security perimeters, organisational and technical interfaces, and system interdependencies that may increase the threat to our systems or the potential impact if risks are not managed.

4. Take a risk-based approach to understand and manage the exposure of our cyberspace

To appropriately and proportionately manage our exposure to cyber security risk, we need to understand: the threats we face, the vulnerabilities or weaknesses in our people or technology, and the potential consequences of a cyber incident affecting our businesses, which includes impact on the operational railway.

5. Have governance for cyber security in our organisations

Successful and effective cyber security programmes require governance, to ensure executive- level support is provided and to define a risk management approach which is aligned to our own business objectives and this strategy. Governance will also ensure we can demonstrate a commitment to delivering cyber security, enable required collaboration by our organisations and provide an avenue for monitoring our progress.

6. Ensure appropriate cyber security management of our systems and their interfaces

Increasing the resilience of our cyberspace requires us to consistently manage the exposure to risk of our systems and their interfaces, by: protecting ourselves and others through cyber security measures for systems and their interfaces to minimise the spread and potential impact of cyber security incidents; and ensuring these include all systems, physical sites, and organisations across the railway, to provide a consistent level of protection.

7. Engage with domestic and international bodies on rail cyber security

Influencing a wide range of interested parties will benefit cyber security on the GB railway. We need to be active in our engagement with others to: promote cyber security good practice throughout the railway; support developments to meet legislative requirements; encourage initiatives supporting investment in cyber security; and ensure the reputation of the rail industry in addressing cyber security risk is positive.

8. Work with third-party suppliers to manage cyber security in our supply chain

Our increasing reliance on our third-party suppliers means we have to manage the risks potentially introduced through our supply chain. We need to work with these delivery partners to improve our combined risk management, and to reduce the vulnerabilities in our systems. We also need to ensure that those working with us procure, design, build, supply, operate, and maintain systems, in a way that meets our requirements. Sharing good practices will align our efforts to achieve a consistent approach for cyber security requirements and assurance efforts.

9. Ensure cyber security measures are applied through the life of our systems

To keep pace with evolving threats to our systems we need to monitor these so we can appropriately build security measures into our systems and maintain and improve these throughout their life. Taking a lifecycle approach will allow us to manage cyber security risk as our systems are: designed and built; operated and maintained; and when they become obsolete.

10. Prepare for and manage cyber security incidents

Cyber security protection includes having our response to a cyber security event or incident prepared. We need to be able to take appropriate measures to: monitor, detect, and alert to minimise the impact of events affecting our systems; have adequate threat intelligence to assess the situation; and limit the damage by providing timely detection of, response to, recovery from, and reporting of, cyber events and incidents.

It is essential that we continue to deliver safe, reliable, and efficient railway services as we face ever evolving cyber threats. As the inevitable digitisation of the railway progresses we must act together, now, to protect our railway cyberspace. Implementation of this strategy is our commitment to take active steps toward delivering our cyber security vision; to assess and improve our organisational maturity in delivering against these industry objectives.

GLOSSARY

Asset
Anything of value to an organisation.

Cyber attack
Exploitation of cyber vulnerability.

Availability
Systems and their data are protected to ensure timely and reliable access to and use of information or systems when required.

Cyberspace
An interactive domain made up of digital networks, that are used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services.

Cyberspace for the railway
Information systems providing services that support delivery of the operational railway, comprising digital assets and their networks that underpin business and operational systems. It includes all related information and all information stored and transferred through these networks.

Cyber threat
The malicious action that can be exercised in and throughout cyberspace, or against it and its fundamental elements. These may be immediate or develop over time.

Confidentiality
Preserving authorised restrictions on information or system access or disclosure to ensure that information or system data cannot be viewed in an unauthorised or undetected manner by individuals, processes or systems.

Cyber security capability
The ability to understand and manage cyber security risk; and protect, detect, alert, respond to and recover from, cyber security breaches, attacks, events, or incidents.

Cyber security event
Indication of a potential breach of information security policy or practices, or failure of security measures or a previously unknown situation that may be security related (may be short- or long-lasting).

Cyber security incident
An unwanted or unexpected cyber security event that has a significant probability of compromising business or railway operations. It may threaten a breach of confidentiality, integrity, or availability of digital assets. May be directly caused by a cyber attack or security breach, or be related to cyber security by other events that result in a cyber security incident(s).

Cyber security risk
A function of the likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Detect
Establishing mechanisms for rapidly identifying an actual or suspected cyber attack and alerting it.

Exposure
Cyberspace having no protection from cyber threat.

Hazard
Potential source of harm.

Information technology
Application of computers to store, retrieve, transmit and manipulate data in the context of a business or other enterprise.

Integrity
Protection of systems and data against improper modification or destruction, ensuring information and systems cannot be modified, deleted, or added to, in an unauthorised, accidental, or undetected manner.

Malware
Malicious software or code that typically damages or disables, takes control of, or steals, information from a computer system. Examples include: botnets, viruses, worms, Trojan horses, spyware, and adware.

Operational railway
The assets, digital and physical, providing direct services to operate the railway or move trains, such as signalling, energy, communications, track, stations, and rolling stock.

Operational technology
Systems which are directly responsible for the functioning of the operational railway, including railway network infrastructure and rolling-stock.

Protect
Install specific security measures to prevent and discourage cyber attack against systems in cyberspace.

Railway stakeholders
A combination or all of railway operators, infrastructure managers, train leasing companies, train owning companies, train builders, train maintainers, and rail industry suppliers that deliver railway services in GB. (Some of these may also be referred to as railway undertakings.)

Respond
Undertake appropriate action in response to confirmed security incidents against systems in the railway cyberspace.

Risk assessment
Process of identification, analysis, and evaluation risk (hazards occurring and the corresponding impacts).

Risk management
A process of co-ordinating activities to direct, and control an organisation with regard to risk; to treat risk and mitigate the adverse impact to which an organisation is exposed.

Safety risk
Likelihood of a hazardous event and its impact on safety.

Situational awareness
Awareness of the operational environment, including knowing what threats the organisation is currently facing, or actively responding to, and against which it needs to enhance protection.

Technology environment
The areas of a business to which the digital assets provide functional services, such as business systems or operational technology, including any interfacing technology providing connectivity between these.

Threat intelligence
Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response

Vulnerability
A weaknesses in systems, system procedure(s), information systems, security measures, or implementations, that can be exploited by a threat source to cause a cyber security event or incident. Vulnerabilities can arise from many sources, including: policy and procedures, architecture and design, configuration and maintenance, physical intrusion, system software and product development, communication and networks, lack of training and awareness.

REFERENCES

HM Government, National Cyber Security Strategy 2016-2021 (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)

Centre for the Protection of National Infrastructure, 2014, SeCuRE: Security Culture Review and Evaluation Tool: A GUIDE FOR ORGANISATIONS (https://www.cpni.gov.uk/system/files/documents/d7/06/SeCuRE-tool-guide-for-national-infrastructure-organisations.pdf)

Centre for the Protection of National Infrastructure, 2014a, CPNI Ongoing Personnel Security: A good practice guide (https://www.cpni.gov.uk/system/files/documents/d0/d2/ongoing-personnel-security-a-good-practice-guide-edition-3.pdf)

Department for Transport, 2016 Rail Cyber Security – Guidance for Industry (http://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf)

European Commission, 2016, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, The Directive on security of network and information systems (NIS Directive) (https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive) and (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC)

European Commission, 2016a, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) and Directive (EU) 2016/680 (See reform of EU data protection rules (http://ec.europa.eu/justice/data-protection/reform/index_en.htm) and (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC) and (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477416887982&uri=CELEX:32016L0680)

European Union Agency for Network and Information Security (ENISA), 2016, Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations (https://www.enisa.europa.eu/publications/good-practices-recommendations/)

t (http://orr.gov.uk/__data/assets/pdf_file/0020/22457/annual-health-and-safety-report-july-2016.pdf)

Technical Strategy Leadership Board, 2012, The Future Railway, the Industrial Rail Technical Strategy 2012 (http://www.rssb.co.uk/Library/Future%20Railway/innovation-in-rail-rail-technical-strategy-2012.pdf)

UK Government, 2015, National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf)

FURTHER READING

Information	Link
HM Government – 10 Steps to Cyber Security	https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
NCSC - Security for Industrial Control Systems (SICS) Framework	https://www.ncsc.gov.uk/guidance/security-industrial-control-systems
NCSC ICS Security Assessment Tool	The tool can be accessed through CiSP or can be requested from NCSC
DHS • **Cyber Security Procurement Language for Control Systems** • **Cybersecurity Capability Maturity Model (C2M2)**	 https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity
IEC62443 Series – Industrial Automation and Control Systems (IACS), Security	http://isa99.isa.org/ISA99%20Wiki/Home.aspx
National Institute of Standards & Technology (NIST) • **CSF (Cyber Security Framework)** • **SP800-30 (Guide for Conducting Risk Assessments)** • **SP800-82 (Guide to Industrial Control Systems (ICS) Security**	NIST Computer Security Resource Center http://csrc.nist.gov/publications/PubsSPs.html
SANS Institute - The Industrial Control System Cyber Kill Chain	http://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
ISO/IEC 27000 Series - Information Security Management System Family of Standards	http://www.27000.org/
DfT Rail Cyber Security – Guidance for Industry	http://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf
CEN-CENELEC Focus Group on Cybersecurity – work underway for EU standardisation	http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.asp

Get in touch

Dennis Rocks, Technical Services Director
Simon Holmes, Head of Cyber and Technology

020 7841 8000
cyber-security@raildeliverygroup.com

Rail Delivery Group Ltd,
2nd Floor, 200 Aldersgate Street,
London EC1A 4HD

www.raildeliverygroup.com

Rail Delivery Group

National Rail

BRITAIN RUNS ON RAIL