AUSTRALIAN RAIL NETWORK CYBER SECURITY STRATEGY

September 2018

RAIL CYBER SECURITY
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ACKNOWLEDGEMENTS

The rail cyber security strategy was facilitated by the Rail Industry Safety and Standards Board (RISSB) following requests for an industry wide approach to manage the increasing cyber threat.

RISSB lead the national rail cyber security program and will continue to work hard with industry to ensure specific initiatives are implemented to mitigate rail cyber security risk.

This strategy has been created with the assistance of the Rail Cyber Security Advisory Group and representatives from industry. RISSB acknowledge the following organisations for their contribution to the development of this strategy:

- Aurizon
- Australian Rail Track Corporation (ARTC)
- CERT Australia
- Kiwirail
- Metro Trains Melbourne
- Queensland Rail
- Office of the National Rail Safety Regulator
- Roy Hill
- Sydney Metro
- Sydney Trains
- TasRail
- Transport for New South Wales
- VicTrack
- Waterfall Security Solutions

Further acknowledgment goes to the Rail Delivery Group (UK) for permission to leverage off their Rail Cyber Security Strategy.

CONTENTS

FOREWORD

Criminal organisations, issue motivated groups and nation states are challenging the security of critical infrastructure around the world. Internet connectivity is making it trivial for these individuals to target Australia's critical infrastructure.

The motivations of these individuals and groups can be characterised as follows:

- Direct financial gain
- Ideology - political or issue motivated
- Industrial espionage
- Prestige
- Revenge

Previously rail systems were not interconnected to business information systems and were comparatively immune to remote malicious or accidental system manipulation by third parties or suppliers. Today the risk landscape is much more complex and difficult to navigate which increases the potential for untreated risks. These untreated risks to critical infrastructure and connected systems can result in significant incidents, interruptions or fatalities.

To address this increased risk to critical rail infrastructure, the Rail industry has asked the Rail Industry Safety and Standards Board (RISSB) to facilitate the development of this Strategy to establish an industry wide approach to managing the increasing cyber threat.

The Strategy covers operational technology such as industrial control systems and business information systems. It focused on addressing risks in a holistic manner across the whole rail industry; including all inter-related systems, and in collaboration with governments, rail infrastructure managers, rail transport operators, and suppliers.

Industry stakeholders are committed to co-ordinating their responses and readiness and developing intelligence sharing approaches to proactively characterise the threat.

STRATEGIC DIRECTIONS

In support of the Strategy, three key strategic directions have been identified for successful implementation of the Strategy by rail transport operators and suppliers.

Build on what exists

Our actions will align with common cyber security frameworks, recognised good practice, and our existing organisational structure and process.

Take responsibility

We will commit to addressing cyber security risks within our organisations and acting to manage the risk.

Work collaboratively

We will work together and share information which improves protection against cyber security threats to the railway.

01
INTRODUCTION

Australia's railways are part of its critical infrastructure. The long, thin supply lines connect cities, ports and mines efficiently, safely and reliably.

Over the last two decades technological advancements, the rise of digital connectivity and Internet of Things have changed rail operations significantly. The rail industry has been on a journey to implement technology in all parts of their operations to provide customers a reliable service at a lower price point.

The benefits of interconnecting business information systems and operational train control systems are increasingly visible. Rail operations become safer, more efficient, and innovative when sophisticated solutions including data analytics and machine learning are applied. These changes do however expose rail systems to increased potential risks and hazards originating from cyber-attacks.

Cyber security is an evolving discipline driving not just the need to identify the cyber risks but to also understand the threats and opportunities these risks present. The impact of an unmitigated threat can cascade and be far reaching:

- damage to rail infrastructure and/or the environment;
- disruption of rail services and consequential costs;
- economic loss;
- increased costs of operation;
- legal and compliance risks including privacy;
- loss of sensitive business or government information; and

Whilst the industry has been making progress towards improving and advancing their cyber security capability, successful implementation of cyber security requires an industry wide approach to the increasing cyber threats. Bold leadership is necessary to create the cultural shift required to extend responsibility for cyber security to the regulator, all infrastructure managers and rail operators, suppliers, and every individual.

RISSB will work with the National Rail Cyber Security Advisory Group to monitor and assist on progressing this strategy through an industry wide action plan.

OUR VISION

Our vision is the elimination of cyber risk resulting in zero cyber-attacks on the Australian rail network.

In addition to establishing defendable architectures and resilient systems, we must commit to improving cyber security skills, awareness and education, and understand the central role this capability has in enabling the digital railways of the future.

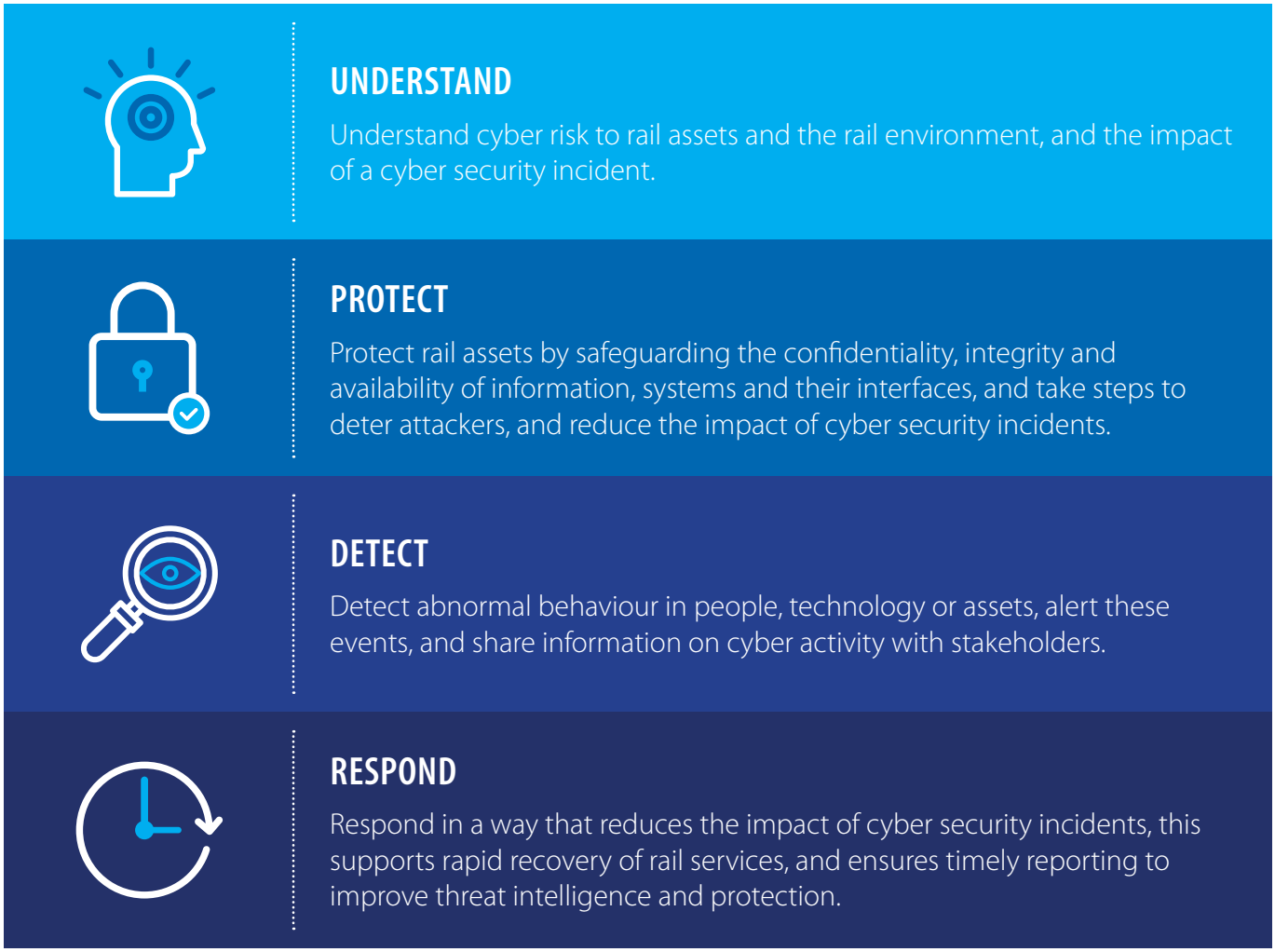
Successful implementation of the Strategy will require a whole-of-industry effort, with collaboration between rail infrastructure managers & rail transport operators, partnerships with suppliers, and assistance from the Australian Government,

The Australian rail industry is widely recognised as one of the safest in the world. We can use this enviable safety record as a model for creating a culture of cyber security that can lead the way and be widely recognised as good practice

As the digitisation of the railway progresses, we must act together now to protect our railway cyberspace.

Acting together, we can ensure strong cyber security capability is at the core of digitally-enabled systems delivering safe, reliable, and efficient rail services.

Figure 1
Description of the key strategic principles



AIM OF THIS STRATEGY

The aim of this strategy is to assist the rail industry participants to manage their cyber risks effectively and work towards solutions to eliminate the risks.

RAILWAY TECHNOLOGY

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

- Business information systems that deliver corporate or enterprise functions and include systems that support and provide interface to rail operations;
- Operational systems that enable the operational railway to reliably and safely function through control of network infrastructure and rolling stock. These can be further divided into:
  - rail control systems that have a direct and immediate effect on safety: and
  - ancillary systems that may have an indirect effect on safety.

Technology is enhancing efficiency and customer service across the railway such 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; and
- IT infrastructure concurrently supporting both business and operational systems

Large and widely dispersed networks can also be very difficult to protect and can provide access points for cyber threats. Increased information sharing across organisational and system interfaces, and greater workforce and third-party interaction with the technology, also increase the digital attack surface of the railway.

WHO SHOULD READ THIS STRATEGY

This strategy is for rail industry executives and management teams. – not just those who are responsible for cyber security. The strategy will also be a valuable guide for government organisations and the industry regulator.

Stakeholders that are responsible for the security and resilience of Australia's operational railway will implement this strategy.

02
RAIL CYBER RISK

The rail environment relies upon digital infrastructure that forms an important part of both the business and operational systems controlling and supporting the rail network.

Cyber related threats, risk the likelihood of an intentional cyber-attack on rail systems is influenced by the attractiveness of the environment, effectiveness of the controls, and threat landscape. Threat intelligence shared by rail transport operators and the Australian Government confirms that attacks are becoming more common and demonstrate that we all have a role to play in enabling better management of these risks.

Sound cyber security is a necessary aspect of a resilient network. It is not an option to simply stop using information and communications technology – the only option is to proactively manage the risk to operations and safety.

The introduction of networked devices with expanded remote access and control capabilities are driving a convergence of IT and OT in rail. This convergence, coupled with the increased linking of different operators and greater demand for services, significantly increases the cyber threat exposure of traditional rail transport networks.

While rail transport operators and engineers possess a wealth of knowledge and experience in ensuring their networks and products are designed and built with safety in mind, they typically have less experience in ensuring the cyber security of their networks and products.

Moreover, since investments in rail networks typically involve significant capital expenditure and long asset lifecycles, these assets may become exposed to new information security threats over the course of their lifetime

Rail transport operators are encouraged to identify the threat sources, threat actors and threat types that may affect the confidentiality, integrity and availability of rail systems. Potential threat sources and actors include: terrorists, criminals, foreign intelligence services, competitors, hackers, activists, malware developers, employees, and contractors. Once the threat sources are identified, systems should be assessed for vulnerabilities to identify the most appropriate ways to introduce security measures to protect the environment through a set of technical, procedural and managerial security controls.

Figure 2
Cyber security activities manage risk to the railway

03
ACHIEVING OUR VISION

OUR MISSION

Our mission is to design and operate safe and secure rail services by appropriately protecting our current and future railway technologies from cyber security risks.

OUR APPROACH

Rail industry stakeholders understand the challenge at hand and how delivering this vision requires unique approaches for every organisation.

The strategy sets out the five objectives that drive the actions required to achieve the vision, remaining adaptable to the commercial drivers, cyber security maturity and risk appetite of each organisation.

These objectives outline what we will accomplish as we progress towards the mission. Ten supporting actions have also been identified to deliver the objectives, based on our approach to improving cyber security.

04
WORKING TOGETHER

To achieve our vision, participants from across the rail industry have corresponding responsibilities and actions. These are depicted in Figure 3 below:

GOVERNMENTS AND REGULATORS

In addition to the operators and suppliers, Government and the Regulator play a vital part in achieving our Cyber Security vision. This can be achieved by close liaison between industry participants and government agencies to:

- Promote public/private collaboration on rail cyber security across Australia and with other countries;
- Support and promote regular cyber security exercises for the rail sector;
- Support the development of a common approach to cyber security including the development of harmonised standards; and
- Support and promote development of a collaborative and open 'incident and near miss' reporting for significant cyber security events.

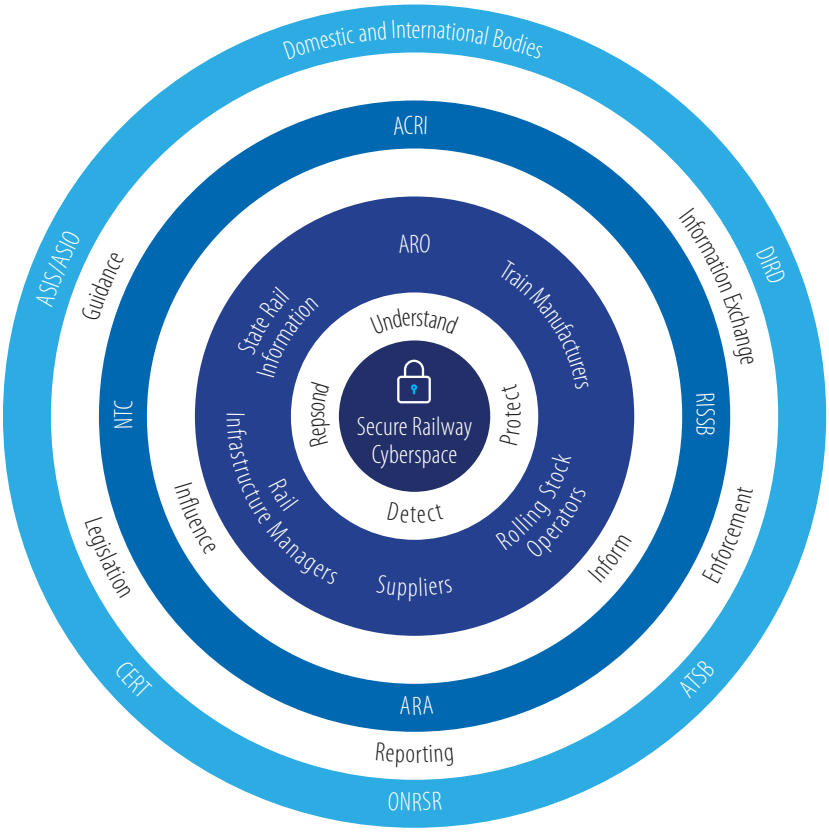


Figure 3
Working together

- Cyber security activities
- Railway stakeholders that deliver the operational railway
- Organisations that provide facilitation and supporting services to the railway
- Organisations that provide rail industry oversight

05
OBJECTIVES

The industry has defined five cyber security objectives and the approach to work towards achieving these objectives.

1.

Our people will understand cyber security risk and act responsibly to ensure that the risks are managed

- Senior management shall accept that they are responsible for information and cyber security risk and commit to systematic and holistic risk management to reduce the hazards resulting from incidents; and
- People in all parts of our organisation shall understand the hazard that cyber security incidents can cause to rail and its importance as critical infrastructure.

2.

We will understand the extent and potential impact of our vulnerabilities on our organisation and those that depend on it

- Our organisation shall understand their cyber security vulnerabilities and the value of operational technology systems, business systems and the information they hold; and
- Our organisation shall assess the cyber security risk to the security and safety of its people, processes and technology.

3.

We will appropriately protect our information, technical systems, physical sites and organisations

- Our organisation shall work collaboratively and holistically with suppliers, other operators and service providers to:
  - protect its people, assets and operations; and
  - regularly assess the adequacy of our cyber security.

4.

Our cyber security capability will be developed and managed to keep pace with evolving threats

- Our organisation shall take measures to keep abreast of evolving security threats and sharing security related information in a trusted manner with other rail operators; and
- Our organisation shall commit to assess cyber security risk as part of purchasing and tendering processes and to protect assets throughout their lifecycle. Our organisation shall work with suppliers to ensure they understand this requirement.

5.

We will be prepared to limit damages from incidents

- Our organisation shall work collaboratively with other operators, our service providers and our suppliers to develop an appropriate security incident response capability; and
- Our industry shall test and improve its ability to respond to incidents.

The table below lists the actions supporting each of our objectives. Each organisation will be responsible for achieving these objectives by developing a more detailed plan that aligns to the objectives. More details on the actions can be found in section six.

Objective	Actions
Our people will understand cyber security risk and act responsibly to ensure that the risks are managed.	A1 Integrate security management systems into corporate governance A10 Provide security guidance for personnel, systems, products and solutions
We will understand the extent and potential impact of our vulnerabilities on our organisation and those that depend on it.	A2 Develop and implement security as a organisation wide strategy A3 Risk management for cyber security and industry stakeholders A9 Contribute to trusted information sharing processes on risks and vulnerabilities A10 Provide security guidance for personnel, systems, products and solutions
We will appropriately protect our information, technical systems, physical sites and organisations	A1 Integrate security management systems in their corporate governance A2 Develop and implement security as a corporate wide strategy A4 Specify our cyber security requirements A7 Create products/solutions that match the cyber security requirements A8 Collaborate to develop and apply technical cyber security standards A10 Provide security guidance for personnel, systems, products and solutions
Our cyber security capability will be developed and managed to keep pace with evolving threats	A5 Regularly review organisational cyber security A7 Create products/solutions that match the cyber security requirements A8 Collaborate to develop and apply technical cyber security standards A9 Share information on risks and vulnerabilities
We will be prepared to limit damages from incidents	As an industry, we will be prepared to limit damages from incidents. A6 Prepare for possible incidents A9 Share information on risks and vulnerabilities

06
OUR GOALS

The following section expands upon those actions which will deliver our objectives. Key activities have been identified for all stakeholders to progress as appropriate in their organisations, and as part of the commitment to this Strategy.

A1

Integrate security management systems into corporate governance

Robust and secure systems do not often happen by accident – they require proactive corporate governance to resource and guide the effort.

We will govern cyber security through our organisation's existing corporate governance processes to monitor the direction, efficiency and the effectiveness of our management of cyber security risks.

Using the existing governance processes will entail using the existing risk management frameworks in each organisation.

A2

Develop and implement security as an organisation wide strategy

Cyber security requires a broadly holistic approach across any organisation. Security plans involve business processes, and more importantly – people. An effective implementation requires security considerations to be part of most business processes and technical systems. Each corporate strategy will include:

- The roles and responsibilities for addressing cyber security risks across our organisation;
- Security awareness for different audiences within an organisation;
- Security training and education for security managers and selected engineers and operators;
- Security management systems and management reporting;
- Security policies, procedures, standards and plans;
- Vulnerability management;
- Technical security configuration and monitoring;
- Security incident detection;
- Security incident response processes;
- Processes to keep informed about the cyber threat environment for the rail industry;
- Processes to inform our industry of the threats we observe targeting our organisations; and
- Design and monitor the security of each important system throughout its lifecycle.

A3

Risk management for cyber security and industry stakeholders

Resources are limited, and so intelligent and focused application of resources is important. Risk management processes are well established techniques to balance the probability and the potential consequences of an incident to determine improvement priorities. Our risk management will consider our customers, other rail industry participants and suppliers as stakeholders.

We will manage our cyber security risks using the same risk management framework used to manage other types of risk. Typically, organisations will integrate cyber risk management for operational technology into existing industrial control system risk assessment methodologies.

A4

Specify our cyber security requirements

We will identify and define our security requirements for processes, services, interfaces and assets.

Our industry's suppliers may not deliver the level of security we desire unless we clearly communicate our expectations. We will communicate these expectations to suppliers and require security to be built into processes, services, interfaces and assets.

A5

Regularly review organisational cyber security

Our organisations appreciate cyber security is a journey within a changing environment. As such, each organisation will take a continual improvement approach to maintaining an adequate level of security. Each organisation will perform the following regular activities as it works to mature its management of cyber security risk:

- Improve organisational security levels;
- Increase the ability to detect incidents in a timely manner;
- review plans to response to an incident;
- reviews of cyber security policy, processes and controls;
- reviews of the threat environment; and
- Liaise with the rail industry and cyber threat information sources.

We will measure and manage the maturity of our cyber security controls, management and governance.

A6

Prepare for possible incidents

Our organisations accept that a cyber security incident may occur. We realise an optimal response to a threat or an incident, can help avoid unnecessary harm, interruptions and expense.

We will:

- Be prepared to respond to a suspected security incident to limit harm to ourselves and our industry peers; and
- Conduct a cross industry exercise to periodically test our ability to coordinate an industry wide response.

A7

Create products/solutions that match the cyber security requirements

Manufacturers, suppliers and service providers will design components, systems and services to meet the security requirements of the industry.

Manufacturers will test of the security of products in the presence of random faults (as per traditional systems reliability engineering practices) and in the presence of malicious cyber security threats.

A8

Collaborate to develop and apply technical cyber security standards

Manufacturers, suppliers and service providers will collaborate on the development of technical cyber security standards. System, performance and interface standards will prescribe security requirements and assumptions where necessary.

A9

Share information on risks and vulnerabilities

All rail industry participants will have a program to detect, assess and remediate security related vulnerabilities. This program will also include these capabilities:

- Suppliers will have a process to receive vulnerability notifications from rail operators, regulators, security testers and other actors known as 'bug hunters';
- Assess the criticality of security vulnerabilities;
- Community of practice to share information;
- Development of security advisories for customers; and
- A system to securely share vulnerability notices within the rail industry.

This approach is akin to the airline industry's principles of sharing information related to maintenance issues and near misses. This approach will contribute to the robustness of cyber security for the rail industry.

A10

Provide security guidance for personnel, systems, products and solutions

All industry participants require awareness and/or training appropriate to their level of accountability, so they can fulfil their responsibility in a competent manner.

Vendors will provide advice on how to securely configure and operate their equipment and services.

GET IN TOUCH

RAIL CYBER SECURITY

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Rail Industry Safety and Standards Board
Level 4, 15 Astor Terrace
Spring Hill, Brisbane QLD 4000

PO Box 518
Spring Hill Qld 4004

www.rissb.com.au

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

RAIL CYBER SECURITY

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

RISSB

RAIL INDUSTRY SAFETY AND STANDARDS BOARD