RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD
ABN: 58 105 001 465

RISSB product for prioritisation

Primary information	
Type of product being suggested:	Guideline
Title of product being suggested:	Rail Cyber Security
Date of suggestion:	28 February 2018
Reason for suggestion:	The extent and sophistication of cyber-attack has increase significantly in recent decades and has moved from being a theoretical and unlikely risk to one that must be managed. AS7770 Rail Cyber Security provides a high-level set of requirements for the management of cyber threat in rail. To further support this Standard a more detailed required is needed to address the factor within Rail Systems. This guideline will be considered as part of the Rail Cyber Security Framework
Railway discipline area:	Safety/Rail Cyber

Scope:

Detailing the required practices to manage the threat of cyber-attacks on the rail network through people which will include:

- Security clearance and access.
- Education and Awareness.
- Risk Culture.
- Getting prepared.
- Risk assessment and control management frameworks.
- Rail personnel and rail systems.
- Operating technology.
- Communicating the cyber risk.
- Data management and storage.
- Authentication.
- Identifying and tracking behaviours.
- Reporting and key indicators.
- Third party.
- Testing the systems.
- Response to threats and attacks.

Train Control Systems, Rolling Stock are not considered in the scope of this document.

Objective:

With the continued introduction of technology and the convergence of information technology and operational technology, rail systems have the risk of being compromised by people. To provide detailed practices to address the threat and vulnerabilities associated with rolling stock systems and providing industry (rail operators, vendors and third party) with specific requirements to assist in the continued progress in the maturity of cyber security risk management.

Hazard identification:			
1	Attacks on the power supply chain – over and under supply.	6	Hackers able to install malware or modify configurations due to lack of configuration controls and access controls.
2	Unauthorised physical access to control systems components, allowing hackers to disable, modify or access OT systems.	7	Hackers able to disrupt systems because type of attack was not considered in original design of the system i.e. lack regular review and upgrading of security controls.
3	Insecure processes and practices for remote access and configuration management lead to systems being vulnerable to the installation of malware during routine maintenance and upgrades.	8	Hackers able to disable OT systems via deleting or encryption of information, due to inadequate access control and lack of isolated backup or system image and configurations.
4	Ability of hackers to impersonate staff due to theft of user name and password credentials via network sniffing.	9	Ability for hackers to socially engineer access via targeting staff with dual access to IT and OT systems (due to lack of training and/or lack of technical controls).
5	Hackers able to compromise supply chain partners' systems giving them knowledge of, or access to, OT systems.	10	Hackers able to compromise supply chain partners' systems giving them knowledge of, or access to, OT systems.

Benefits:

Safety

Rail cyber-attack has the potential to result in any of the following outcomes:

- Loss of life.
- Serious injury to passengers and staff.
- Other threats to safety, including injury.
- Disruption to network operations.
- Economic loss to operators, suppliers and the wider Australian community.
- Reputational damage to rail organisations and government.
- Loss of and /or corruption of commercial, sensitive and operational information.
- Physical damage to infrastructure.

Ensuring that rail systems are protected from/and are resilient to cyber-attacks provides assurance to rail transport operators, customers and the community.

Interoperability[i] / harmonisation[ii]

Cyber security threat has been managed through individual organisations at various levels. To leverage off the work undertaken and build on future insight will allow industry to work at a national level on the risk. This product which will support the national standard (AS7770) will address the various systems utilised across the network through interoperability of system management.

Financial

The cost of a major cyber-attack on the national rail network would eventuate in a high cost on the Australian economy whether it be delays to peak metro services. port or transportation of goods. Innovation and technology will continue to evolve and be taken on in rail and therefore the investment need to be protected.

Environmental
Potential of rail incidents specifically involving dangerous goods and bulk commodities.
Impacts:
Minimum impacts as this would be supporting AS7770. Industry need a rail cyber security framework and this document will one of many that will support individuals' element of the rail system. Groups are already formed and will be available to develop.

i Interoperability - the ability of a process, system or a product to work with other process, systems or products (aka compatible systems through managed interfaces).

ii Harmonisation - the act of bringing into agreement so as to work effectively together (aka uniformity of systems).