SMART RAILWAYS… OR NOT SO SMART: A CYBER SECURITY PERSPECTIVE

Raymond C Frangie[1] MInfoSysSec(*CSturt*), MACS CP (Cyber Security), CISSP, CEH, ECSA, LPT, Alan Mihalic[1] CISSP, ISSAP, ISSMP, CISM, Travis Chehab[1] BE BSc RBP ISO27001LA, John Kan[2] BE (Hons), Chi Ping Luk[3] BSc MSc MIET CEng, Sivanandan Perinpacumarasamy[3] BEng, MBA.

[1]*NDY Cyber, Norman Disney & Young (NDY), a Tetra Tech Company, AUSTRALIA*

[2]*ICT & Security Global Specialist Group, Norman Disney & Young (NDY), a Tetra Tech Company, AUSTRALIA*

[3]*NDYLTK Rail Pty Ltd, AUSTRALIA*

Corresponding Author: R.Frangie@ndy.com

SUMMARY

Welcome to a world where smart railways are here and now. Real-time monitoring, embedded sensors, driverless trains, automated signalling and train control, Internet of Things (IoT), instant travel disruption alerts, and more. Operators not only need to continue to focus on operating railways, but now must monitor and protect all this connected infrastructure from a cyber-attack. The more connections, the more cyber threat attack vectors, the more potential for exploitable vulnerabilities, the more risk of a cyber-attack occurring.

As the owner or operator responsible for the railway, how often do you perform risk assessments specific to cyber and/or information security? How confident are you of being proactive towards a cyber-attack? Are you able to identify, classify and/or mitigate a cyber security related risk? Does your risk management framework allow for accurate classifications of cyber security related risks in line with industry best practices? Will you be non-compliant and subject to financial penalties from regulations and/or legislation such as the Australian Notifiable Data Breaches (NDB) Scheme?

The aim of this paper is to shallow dive into information and cyber security for rail networks and operations, providing advice into protecting a rail network's infrastructure from cyber security threats, to the same high level expected by all involved.

1. INTRODUCTION

Travelling the world's metro systems in places such as Dubai [1], Copenhagen [2], Lille [3], Vancouver [4], Santiago [5], Lima [6], Sao Paulo [7] and through the numerous airports around the world, what do you see becoming more common? This train has no driver! Most people will be in awe of the technology, the punctuality of the train service, the state of the country and how such technology seems to just run without any issues and wonder why we never had this technology sooner. A rail engineer would see the system as a marvel of railway engineering that they would be more than proud of. A rail executive would see the system as a great way to achieve organisational objectives while lowering organisational expenditures due to less overheads and more automation. Railway stakeholders and shareholders would see great investment opportunities due to both the marvel of engineering and the low operating costs.

In contrast however, a cyber security professional views these environments as a Pandora's box of potential critical vulnerabilities and wonders when, not if, these systems will join a growing global list of breached systems, creating issues such as delays, derailments [8], and/or in some cases, even death [9].

In 2014, the American Public Transportation Association (APTA) warned municipalities of attacks via its position paper that stated, "cyber-attacks can destroy a transit agency's physical systems, render them inoperable, hand over control of those systems to an outside entity or jeopardise the privacy of employee or customer data" [10]. Since the APTA statement, more than 6.4 billion control systems have connected online, estimated to be over 20 billion by 2020 [11]. What this statement fails to identify however, is the potential damage which assignment of a monetary amount is not possible; reputational damage. In the words of Warren Buffet,

"It takes twenty years to build a reputation and five minutes to ruin it".

Modern transit systems are increasingly dependent on a variety of integrated information technology systems and therefore are intrinsically "at risk" to a wide spectrum of cyberthreats. This paper shall provide a basic high-level insight into how, by simply following certain cyber security measures, standards, frameworks and/or guidelines, a transportation organisation can increase their information and/or cyber security maturity, significantly reducing their exposure to such cyber threats.

2. CYBER SECURITY VS INFORMATION SECURITY

Prior to proceeding, given the usage of the following terms synonymously throughout this paper, it is best to address the confusion between Cyber Security and Information Security.

According to the National Institute of Standards & Technology (NIST), Internal Report 7298 Revision 2, dated May 2013 [12], cyber security is the ability to protect or defend the use of cyberspace from cyber-attacks. Cyberspace is a global domain within the information environment, consisting of the interdependent network of information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. A cyber-attack is an attack, via cyberspace, targeting an enterprise's use of cyberspace to disrupt, disable, destroy, or maliciously control a computing environment or infrastructure; and/or destroy the integrity of the data and/or steal controlled information.

Information Security on the other hand is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

3. TARGET OF ATTACK

When attackers wish to attack a system, cause havoc, demand a ransom, or even cause harm, irrespective of whether an attacker is a 14-year old child [8], or a nation state, such attacker will aim to target one or more of the three pillars of information security, known as the Information Security C.I.A Triad. C.I.A in this instance, is subsequently an abbreviation for the terms Confidentiality, Integrity, and Availability.

Figure 1: The Information Security C.I.A Triad

There are many variants and similarities in the definitions of these three pillars, however using the definitions from the National Institute of Standards and Technology:

- **Confidentiality:** Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [13].
- I**ntegrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [14].
- **Availability:** Ensuring timely and reliable access to and use of information [15].

Notwithstanding the official definitions above, a loss of confidentiality is further known as the unauthorised disclosure of information, such as customer data, employee data, network designs, system configurations, and/or other Personally Identifiable Information (PII). With respect to integrity, a loss of integrity is known as the unauthorised modification or destruction of any type of information, and finally, a loss of availability, is the disruption of access to, or use of, information or an information system.

Let us now put a rail perspective on this. Consider confidentiality; customer information, such as name, physical address, email address, or more critical data such as credit card information used for automated top up of fare collection systems. How

about employee information such as the trains a specific employee is to operate, or which guard is operating which train, or which train will have a ticket inspector or plain clothes police officer on it. Alternative critical information would be track plans and/or layouts, signal deployment configuration and/or plans, designs of the railway network, or even detailed technical configuration as to how trains operate across the network, or worse, login credentials to train operation control systems. What would happen if this information leaked to the Internet, or sold off on the dark web or black market? To the naked eye, this information might not seem or sound valuable, but for an attacker, any intelligence is valuable intelligence.

How about the integrity of information? Is that command to this signalling device from the train operation control centre, really coming from the train operation control centre? How can the signalling equipment be sure that the command it is receiving is not by an attacker lurking within, or external to, the network? Case in point; the 14-year old teenager who converted a TV remote control to send commands to track points, turning the tram system into his personal train set, triggering chaos and derailing four vehicles in the process, injuring passengers [8]. Where was the integrity checking in this scenario? Why was the signalling equipment allowed to process the command and not be able to explicitly verify that the command received was authentic? Does this feature not exist or is it simply not implemented? Will future changes to signalling infrastructure by upgrading ageing signalling systems to computer-based signalling systems be susceptible to the same form, or more advanced forms, of attack? [16] Simply because a computer was not involved in this attack does not mean it was not a cyber-attack. Events like these highlight the need for more innovation by the transportation industry to ensure implementation of cyber security is within every phase of the system development life cycle (SDLC), well before the equipment manufacturing and/or implementation stages.

Of the three pillars of the Information Security Triad, the pillar of Availability would be the most targeted by an attacker, given that it could be the easiest of the three to attack. Consider this scenario; attacker infiltrates train display information removing the availability for passengers to determine which platforms they need to go to, causing havoc across the station, frustration among passengers, subsequently causing damage to the reputation of the rail organisation due to not being able to manage passenger flow and information correctly. With social media and its power to make messages and news go viral, reputational damage is not only dangerous but it is very real. It's not like this sort of attack and scenario has not happened before [17, 18]. How about another scenario? An attacker, using a modified access / RFID / proximity card reader device, captures an employee's access card details simply by walking past them, creates a duplicate card with their details, infiltrates a rail networks operations control room, connects a laptop to a system within the control room, manipulating track points and controls [33]. We all know what could happen here if this occurred.

While there are numerous scenarios that an attacker may create to attack the confidentiality, integrity, or availability of a railway network, it is also a common misconception that many cyber-attacks are external, and if the railway network protects its external boundaries via a firewall or some other security protection method, they will be unaffected and protected from cyber threats and/or attacks. Transit agencies, just like any other organisation, are susceptible to attacks from internal sources, such as a disgruntled employee. Although, an attack from an internal source has a higher probability of success and a greater potential for damage, given the level of access and knowledge an insider may possess, it is imperative that organisations no longer assume that simply placing a firewall or other security protection method on its boundaries is sufficient.

In 2016, the Australian Cyber Security Centre (ACSC) issued its Annual Threat Report [19]. This report showed that the Computer Emergency Response Team (CERT) of Australia responded to just shy of 15,000 cyber security incidents. Over 10% of these were incidents in Australia targeting the transportation industry. In April of 2017, Symantec also released Volume 22 of its Internet Security Threat Report [20] which states that of the Top 10 Sectors breached by number of incidents in 2016, the Transportation and Public Utilities Sector ranked 5th with just over 7% of all attacks attributed to this sector.

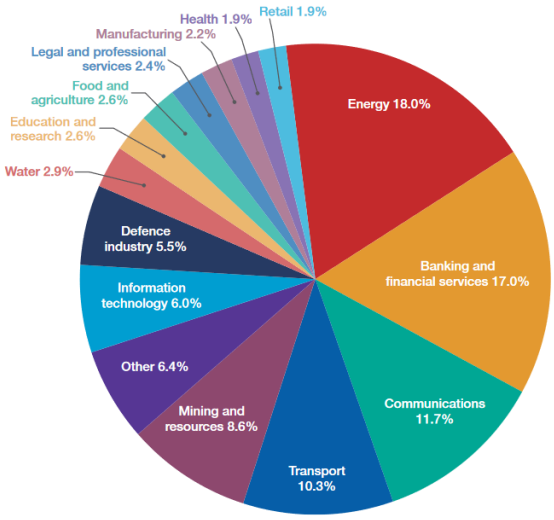

Figure 2: ACSC Threat Report 2016 Incident Breakdown

Top 10 sectors breached by number of incidents

Services was the industry most affected by data breaches in 2016.

Rank	Industry	Breaches	Percent
1	Services	452	44.2
2	Finance, Insurance, & Real Estate	226	22.1
3	Manufacturing	116	11.3
4	Retail Trade	84	8.2
5	Transportation & Public Utilities	75	7.3
6	Wholesale Trade	32	3.1
7	Construction	20	2.0
8	Mining	8	0.8
9	Public Administration	6	0.6
10	Nonclassifiable Establishments	3	0.3

Figure 3: Symantec ISTR Volume 22 Top 10 Sectors breached by number of incidents in 2016

Not all is doom and gloom however. Rail systems and networks are known to demonstrate some of the highest levels of systems engineering in the current age of integration complexity. This same level of rigour must apply to cyber security. Organisational information security and/or cyber security policies must be clear in terms of critical elements, such as primary business processes, resources, and personnel. Support for such policies must be via all levels of the organisation, from the top to the bottom, and by assurance and technical procedures, ensuring system integrity and robustness, frequent active vulnerability scanning and/or continuous passive vulnerability scanning, heuristic and/or behavioural analysis, response planning, and penetration testing.

4. WHERE TO BEGIN

As with any form of technology or industry, specific industry best practices, standards, guidelines, and/or frameworks exist to assist organisations in standardising their environments and ensuring implementation of best practices. When it comes to cyber security, it is no different; there are numerous standards, guidelines, and frameworks specifically designed for the securing of environments, some even specific to certain industries; example being the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard, designed to secure the assets required for operating North America's bulk electric system. With respect to the transportation industry, specifically rail, the Rail Industry Safety and Standards Board (RISSB) currently has a draft version of Australian Standard (AS) 7770:2018, Rail Cyber Security Safety Standard [2021], out for public consultation. This standard, which is a great start to defining cyber security for the rail industry, references many of the common frameworks currently known and in use globally for many years within the cyber and information security industries. Such frameworks include the

- International Organisation for Standardisation (ISO) 27000 Series, specifically ISO 27001:2015 [22] and its associated 27002:2015 [23] standard,
- National Institute of Standards and Technology (NIST) Cyber Security Framework [24] and numerous other NIST Special Publications,
- Australian Signals Directorate (ASD) Essential Eight Strategies to Mitigate Cyber Security Incidents [25], and the
- Centre for Internet Security (CIS) Critical Security Controls for Effective Cyber Defence [26], amongst many others.

Following any of the frameworks to secure an environment may seem daunting at first, with organisations either giving it to their IT department to look after, or placing it in the too hard basket. Gone are the days when companies could pass the headaches of cyber security to the IT department, as it is a fundamental business issue not an IT issue [27].

For organisations that are looking to secure their environments but are unsure as to where to start, it is always best to start with the fundamentals. Rather than deep diving into any one of the numerous frameworks, and feeling overwhelmed, start with simple guidelines. The first five of the CIS Top 20 Critical Security Controls [26] and the Essential Eight from the Australian Signals Directorate [25] are the best to significantly lower the risk of cyber threats for an organisation. So much so, that the first five CIS Controls are often referred to as providing cyber security "hygiene", with studies showing that implementation of the first five CIS Controls provides an effective defence against the most common cyber-attacks (~85% of attacks) [28]. The following sections shall explain these simple guidelines in further detail.

5. THE CIS CONTROLS – FIRST FIVE

The Centre for Internet Security (CIS) Critical Security Controls (CSC), are a prioritised set of actions that protect an organisation's critical systems and data from the most pervasive cyber-attacks. These controls embody the critical first steps in securing the integrity, mission, and reputation of an organisation [28].

The first five of the CIS Controls are as follows.

5.1 CIS CSC #1 - Inventory of Authorised and Unauthorised Devices

Organisations must actively manage (inventory, track, and correct) all hardware devices on the network so that access is provided only to authorised devices, and unauthorised and unmanaged devices are found and prevented from gaining access [29].

No longer is it safe to simply have a spreadsheet, or document, that details all the assets on the network or within an environment. Such document is already out of date before it is complete. Commissioning of automated scanning systems that continuously scan the environment for devices is highly recommended. Known assets should be marked as a "known device" to not generate alerts (or generate alerts if the device has not checked in for a certain period and is not in a maintenance mode state), however if the automated system detects an unknown piece of hardware on the environment, then automated action where possible, along with alerts must be initiated and investigations taken place to ensure the integrity and security of the environment.

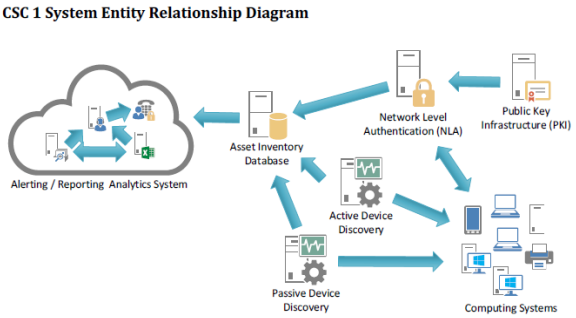

Figure 4: System Entity Relationship Diagram on implementation of Critical Security Control #1

5.2 CIS CSC #2 - Inventory of Authorised and Unauthorised Software

As is the case with the first of the CIS Controls, organisations must actively manage (inventory, track, and correct) all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution [29].

Attackers continuously scan target organisations looking for vulnerable versions of software that are remotely exploitable. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch is available from the software vendor. Without proper knowledge or control of the software deployed in an organisation, organisations and defenders cannot properly secure their assets [29].

Amongst many other frameworks, standards and guidelines mandating the implementation of such security control, this control operates hand in hand with one of the Australian Signals Directorate's Essential Eight controls, specifically being Application Whitelisting [25].

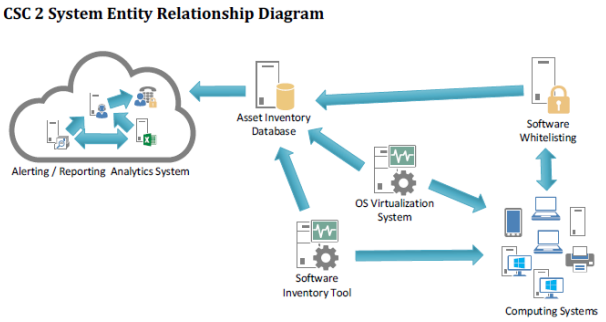

Figure 5: System Entity Relationship Diagram on implementation of Critical Security Control #2

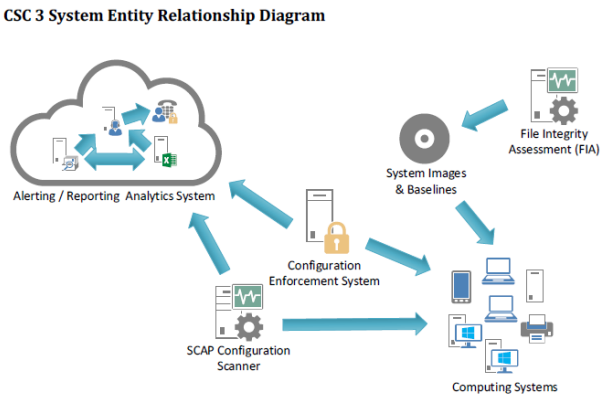

Figure 6: System Entity Relationship Diagram on implementation of Critical Security Control #3

5.3 CIS CSC #3 - Secure Configuration for Hardware and Software

Implementation of the third of the CIS Controls is without question. Organisations must, for basic cyber security hygiene, establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

Typically geared to ease-of-deployment, ease-of-use and not security, are default configurations for operating systems and applications as delivered by manufacturers and resellers. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state [29]. This not only applies for servers, laptops, workstations, and mobile devices, but for all types of equipment, be it signalling devices, automatic protection systems, and practically, anything that has a network connection or broadcasts on radio frequencies.

The Centre for Internet Security (CIS) has numerous system and device hardening benchmarks across a broad range of hardware and software, obtainable for free, to assist organisations in building secure configurations for their infrastructure.

Amongst many other frameworks, standards and guidelines mandating the implementation of such security control, this control also operates hand in hand with more than one of the Australian Signals Directorate (ASD)'s Essential Eight controls, specifically being User Application Hardening, Patch Applications, and Patch Operating Systems [25].

5.4 CIS CSC #4 - Continuous Vulnerability Assessment and Remediation

Given that the cyber security threat landscape is continuously and frequently changing, organisations must continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers [29].

As part of a program to increase an organisations information security maturity, it is no longer prudent to just scan environments for vulnerabilities annually or every six months or every quarter or even every month. Sub Control 4.1 of CSC #4 states that organisations must run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritised lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk [29].

Implementation and obtaining of threat intelligence information to assist in the determining of threats specific to an organisation, via the numerous tools and methods available, is highly recommended. Researching known threats to the systems, devices, hardware, industrial control systems, etc., within an organisation's environment is imperative to understanding cyber threats that may potentially be engaged in an attack against the organisation.

CSC 4 System Entity Relationship Diagram

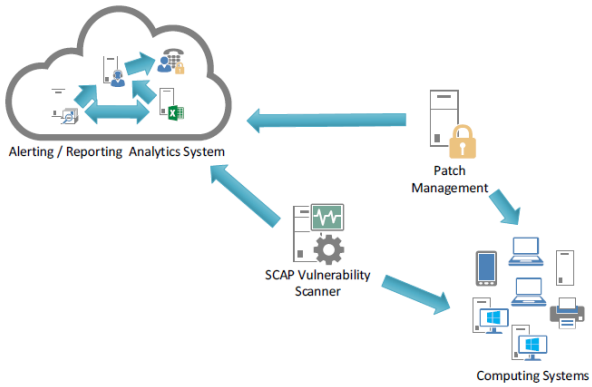

Figure 7: System Entity Relationship Diagram on implementation of Critical Security Control #4

CSC 5 System Entity Relationship Diagram

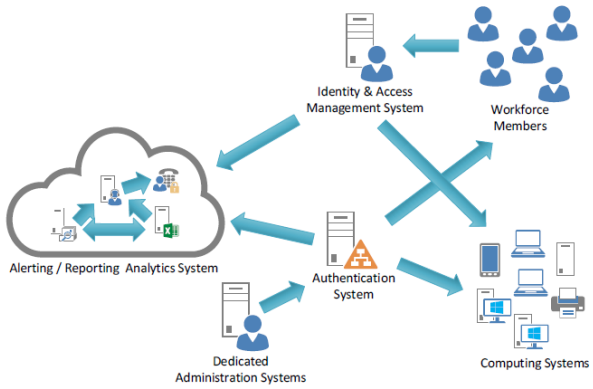

Figure 8:System Entity Relationship Diagram on implementation of Critical Security Control #5

5.5 CIS CSC #5 - Controlled Use of Administrative Privileges

The last of the first five controls is as critical to the other four in protecting environments from cyber-attacks. The misuse of administrative privileges is a primary method for attackers to spread inside a target organisation.

Organisations must commission processes and tools to track, control, prevent, and/or correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications [29]. With numerous methods of attack for capturing and/or fooling a user to inadvertently release their credentials to an attacker, minimising administrative privileges and only using administrative accounts when required, notwithstanding the implementation of focused auditing on the use of administrative privileged functions, monitoring for anomalous behaviour is key. Organisations should also look at implementing dedicated administrative workstations, isolated from a general user workstation, implementing dedicated administrative user accounts along with multi-factor authentication where there is a need for administrative privileges to perform a task.

Amongst many other frameworks, standards and guidelines mandating the implementation of such security control, this control also operates hand in hand with more than one of the Australian Signals Directorate's Essential Eight controls, specifically being Restrict Administrative Privileges, and Multi-Factor Authentication [25].

6. CONCLUSION / RECOMMENDATIONS

From implementing cyber security controls, to designing policies, plans, procedures, and/or processes for a top-down policy approach, or performing operational tasks such as vulnerability assessments, penetration tests, environment audits, for a bottom-up approach, or even performing cyber security centric risk assessments, this paper is simply a very high-level insight into the requirements of protecting all environments, increasing an organisations information security maturity, and not just user environments from cyber-attacks.

With 93% of cases showing hackers only taking minutes to breach environments, companies taking weeks or even months to discover they have been breached [30], and studies showing that US companies took an average of 206 days to detect a data breach [31], it is imperative that everyone, not only the rail industry, work together in securing their environments from attackers. Security is everybody's responsibility. Although it is not possible to eliminate risk entirely, the establishment of risk management strategies, appropriate governance and compliance modelling, and the adherence to information security maturity level guidance, will ensure the identification, classification, and mitigation of cyber security risks in accordance with industry best practices.

Notwithstanding the basic guidelines above, organisations aiming for cyber security readiness and preparedness should include the following five pillars of cyber security readiness according to the Australian Computer Society [30]:

6.1 Education and Awareness

First, it is essential that cyber security forms part of the conversation in every organisation, from the lunch room to the boardroom. Only through keeping cyber security front of mind can it form part of the decision-making process, infrastructure investment, and regulatory and governance requirements [30].

Continuous security awareness and training procedures should take place on a frequent basis, with quizzes or assessments provided to personnel to ensure competence in such facets of information and/or cyber security.

6.2 Planning and Preparation

As stated earlier in this paper, a cyber security incident is no longer an 'if' but a 'when', and to that end, preparation is essential. This can include management systems, best practice policies, IT auditing, and dedicated staff responsible for cyber security operations [30].

Cyber security readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cyber security threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, has incident response plans in place in the event of a breach, and clear business continuity plans to minimise any loss [30].

6.3 Detection and Recovery

When a breach happens, the quicker the detection and response, the greater the chance of minimising loss – be it financial, reputational, or otherwise [30].

Importantly, the preservation and analysis of device audit logs that can help identify how the breach happened, and thus future prevention, is part of the recovery process. It is not enough to just close the hole; an understanding of how the breach occurred can lead to preventing other, similar, breaches [30].

6.4 Sharing and Collaboration

Collaboration is essential to mitigating current and future risks. Sharing the results of your breach analysis with government and industry can help stop a known attack vector hitting other organisations. In turn, organisations may be able to prevent an exploit by learning from a breach that another organisation shared. Organisations should also consider joining or providing information to an Information Sharing and Analysis Centre (ISAC) [30]. For the Rail Industry, consider joining the Surface Transportation Information Sharing and Analysis Centre (ST-ISAC) and subscribing to the Transit and Rail Intelligence Awareness Daily (TRIAD) report [32].

6.5 Ethics and Certification

It may initially seem a less practical pillar, but the difference between a 'white hat' hacker and 'black hat' hacker is mindset. In any company or organisation, ethics plays a role and should be of concern when it comes to cyber security. While some sectors, such as defence, will have their own means to vet credentials, for an industry as diverse and skilled as rail and transportation it helps if professionals can demonstrate adherence to a code of ethics through membership of a professional institution [30] if not already.

Working with teams that contain cyber security and ICT certified professionals, inclusive of rail focused engineers who are members of numerous professional bodies, bound by codes of ethics and conduct, will assist organisations with top-down policies all the way through to bottom-up approaches.

Engaging such teams shall allow organisations to continuously understand their cyber security risks, further understanding how to remediate and/or mitigate identified cyber security risks.

7. REFERENCES

1. Railway Technology. (n.d.). Dubai Metro Network. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/dubai-metro/

2. Railway Technology. (n.d.). Copenhagen Metro, Light Rail and Metro Project, Denmark. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/copenhagen/

3. Railway Technology. (n.d.). Lille VAL. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/lille_val/

4. Railway Technology. (n.d.). Vancouver SkyTrain. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/vancouver/

5. Railway Technology. (n.d.). Santiago Metro. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/santiago-metro-new-lines/

6. Railway Technology. (n.d.). Lima Metro. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/lima-metro/

7. Railway Technology. (n.d.). São Paulo Metro. (Kable Intelligence Limited) Retrieved February 2018, from Railway Technology: https://www.railway-technology.com/projects/saopaulometro/

8. Leyden, J. (2008, January 11). Polish teen derails tram after hacking train network. Retrieved February 2018, from The Register: https://www.theregister.co.uk/2008/01/11/tram_hack/

9. National Transportation Safety Board. (2009). Railroad Accident Report - Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station Washington, D.C. Washington D.C: National Transportation Safety Board Retrieved February 2018, from https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1002.pdf

10. American Public Transportation Association. (2014). Cyber security Considerations for Public Transit. American Public Transportation Association, Enterprise Cyber Security Working Group. Washington D.C: American Public Transportation Association. Retrieved February 2008, from http://www.apta.com/resources/standards/Documents/APTA%20SS-ECS-RP-001-14%20RP.pdf

11. Mitchell, O. (2016, December 4). Your Train Has Just Been Hacked. Yes, This Just Happened. Retrieved February 2018, from Medium: https://medium.com/@olivermitchell/your-train-has-just-been-hacked-yes-this-just-happened-bd6364b99d04

12. National Institute of Standards and Technology. (2013, May). Glossary of Key Information Security Terms. (R. Kissel, Ed.) Gaithersburg, MD, United States of America. doi:10.6028/NIST.IR.7298r2

13. National Institute of Standards and Technology. (n.d.). Confidentiality. Retrieved February 2018, from Information Technology Laboratory - Computer Security Resource Centre: https://csrc.nist.gov/Glossary/?term=3591

14. National Institute of Standards and Technology. (n.d.). Integrity. Retrieved February 2018, from Information Technology Laboratory - Computer Security Resource Centre: https://csrc.nist.gov/Glossary/?term=4875

15. National Institute of Standards and Technology. (n.d.). Availability. Retrieved February 2018, from Information Technology Laboratory - Computer Security Research Centre: https://csrc.nist.gov/Glossary/?term=3103

16. Westcott, R. (2015, April 24). Rail signal upgrade 'could be hacked to cause crashes'. Retrieved February 2018, from BBC News Technology: http://www.bbc.com/news/technology-32402481

17. Graham, C. (2017, May 23). Cyber-attack hits German train stations as hackers target Deutsche Bahn. Retrieved February 2018, from The Telegraph: http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/

18. Liptak, A. (2016, November 27). Hackers are holding San Francisco's light-rail system for ransom. Retrieved February 2018, from The Verge: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cyber security-muni

19. Australian Cyber Security Centre. (2016). 2016 Threat Report. Canberra, ACT, Australia. Retrieved February 2018, from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

20. Symantec. (2017, April). Internet Security Threat Report. (Volume 22). Retrieved February 2018, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

21. Rail Industry Safety and Standards Board. (2017, October 30). AS7770:2018 Rail Cyber Security Safety Standard (Public Consultation Draft). Kingston, ACT, Australia. Retrieved February 2018, from https://www.rissb.com.au/wp-content/uploads/2017/10/AS-7770-Rail-Cyber-Security-V2.0-Public-Consultation.pdf

22. Standards Australia. (2015). AS ISO/IEC 27001:2015 - Information technology - Security techniques - Information security management systems - Requirements. Retrieved February 2018, from SAI Global - Store: https://infostore.saiglobal.com/en-au/Standards/AS-ISO-IEC-27001-2015-1797414/

23. Standards Australia. (2015). AS ISO/IEC 27002:2015 - Information technology - Security techniques - Code of practice for information security controls. Retrieved February 2018, from SAI Global - Store: https://infostore.saiglobal.com/en-au/Standards/AS-ISO-IEC-27002-2015-1797415/

24. National Institute of Standards and Technology. (2017, December 30). Framework for Improving Critical Infrastructure Cyber security. (Version 1.1 Draft 2). Gaithersburg, MD, United States of America. Retrieved February 2018, from https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

25. Australian Signals Directorate. (2017, February). Essential Eight Explained. Canberra, ACT, Australia. Retrieved February 2018, from https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

26. Centre for Internet Security. (n.d.). CIS Controls, 6.1. Retrieved February 2018, from Centre for Internet Security: https://www.cisecurity.org/controls/

27. Campbell, N. (2017, October 11). Cyber Security is a Business Risk, not just an IT Problem. Retrieved February 2018, from Forbes: https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/#724119567832

28. Centre for Internet Security. (n.d.). CIS Controls - Download the First 5 CIS Controls Guide. Retrieved February 2018, from CIS - Centre for Internet Security: https://learn.cisecurity.org/first-five-controls-download

29. Centre for Internet Security. (2016, August 31). Critical Security Controls for Effective Cyber Defence. (Version 6.1). East Greenbush, NY, United States of America. Retrieved February 2018

30. Australian Computer Society. (2016, November). Cyber security Threats Challenges Opportunities. Sydney, NSW, Australia. Retrieved February 2018, from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cyber security_Guide.pdf

31. Irwin, L. (2018, February 21). How long does it take to detect a cyber-attack? Retrieved February 2018, from IT Governance USA: https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/

32. Surface Transportation Information Sharing and Analysis Centre. (n.d.). 24/7 Threat Warning, Incident Reporting, and Analysis. Retrieved February 2018, from Surface Transportation Information Sharing and Analysis Centre: https://www.surfacetransportationisac.org

33. Hacker Warehouse. (n.d.). Proxmark3 RDV2 Kit. Retrieved February 2018, from Hacker Warehouse: https://hackerwarehouse.com/product/proxmark3-rdv2-kit/