Understanding Cyber-Resilience Approaches and Compliance Levels within the Railway Sector

Cybersecurity continues to hold paramount importance in the railway industry due to the integral role of technology in meeting commercial and operational demands.

Recognising the critical nature of this issue, RISSB and Griffith University teamed up to create the Railway Cybersecurity Survey. The survey aimed to understand rail company approaches in cybersecurity and where our industry's general maturity lies.

The report provides valuable insights into the cyber compliance levels, including the following four main recommendations:

1. Foster continuous improvement and systematic evaluation of cybersecurity practices
2. Establish cross-functional collaboration for improved authentication and incident documentation
3. Maintain up-to-date cybersecurity training and post-incident analysis
4. Implement RISSB Standard AS 7770 for network security and proactive cybersecurity culture.

These recommendations will help inform RISSB's thinking about how we can better support rail industry's cybersecurity efforts.

Cybersecurity Resilience in Australian Railways

Understanding Cyber-Resilience Approaches and Compliance Levels within the Railway Sector

By Ojaswini Malhotra for RISSB | June 2024

Executive summary

This survey-based research delves into cybersecurity within the railway sector, aiming to understand the cyber-resilience strategies embraced by rail transport operators (RTOs). The primary focus lies in comprehending the outlook of Australian railways and their approaches to cybersecurity, assessing the industry's maturity against the RISSB cybersecurity framework and Cybersecurity Maturity Model Certification (CMMC)[1].

Survey methodology

The survey, distributed through RISSB newsletters and direct emails to rail officials, garnered insights into cybersecurity practices within the railway industry. Participants contributed anonymously, providing valuable data for analysis.

Cybersecurity compliance levels

Survey questions were categorized into five levels, ranging from basic to advanced cyber-hygiene practices. Results indicated that:

- 34.45% of the railway industry complies with basic cyber-hygiene practices (Level 1).
- Level 2 (intermediate) practices are followed by 38.1% of the industry, surpassing Level 3 (good) practices at 30.79%.
- Notably, the industry exhibits the lowest compliance with Level 5 (advanced) practices, with an efficiency of 27.56%.

Documenting, reviewing, and optimizing protocols

Organizations demonstrate proficiency in documenting and optimizing cybersecurity practices but show reluctance in reviewing security protocols. While risk mitigation efforts are evident, insufficient attention is paid to reviewing risk procedures and practices.

Authenticating and highlighting cyber-risk context

Effective authentication measures coupled with robust incident tracking and reporting correlate with enhanced threat detection. Conversely, poor implementation of these practices results in a subpar risk context for railway operations.

Cybersecurity training and funding

The study underscores the significance of effective training and adequate funding for cybersecurity. Mere funding increases do not guarantee a cyberthreat-free environment; instead, the efficacy of training in responding to cyber threats is pivotal for organizational resilience.

Cyber-risk assessment plans and security controls monitoring

A positive correlation exists between monitoring security controls, managing boundary communications, and developing risk assessment plans. However, some organizations prioritize rigorous security control monitoring over boundary communications management.

Recommendations for enhanced cybersecurity

While adhering to RISSB cybersecurity standards is commendable, adherence to the specific practices put forward in AS 7770, *Rail Cyber Security* Standard and *Rail Cyber Security for Rolling Stock* and *Train Control Systems – Code of Practice* is advised to bolster cybersecurity resilience. These practices encompass integrating security into rail systems, prioritizing controls, and maintaining ongoing vigilance against cyber threats. Embracing these practices ensures a more robust implementation, fostering optimal cyber-secure environments aligned with industry guidelines.

[1] CMMC is a framework that integrates cybersecurity best practices from various standards, organized into five levels and domains.

Defined terms and abbreviations

Generic rail industry terms and definitions are provided in the RISSB Glossary
https://www.rissb.com.au/products/glossary/

Defined terms with specific or unique application within this white paper are listed:

a) blacklisting

identifying and blocking or denying access to known malicious entities or activities by maintaining a list of unauthorized or harmful items, such as malicious IP addresses, software applications, or specific types of traffic

b) CUI

controlled unclassified information, i.e. any information that law, regulation, or government-wide policy requires safeguarding or dissemination controls

c) FCI

non-public information provided for the government under a contract to develop or deliver a product or service to the government, excluding information provided to the public or simple transactional information

d) NIST

National Institute of Standards and Technology

e) RTO

rail transport operator

f) TTP

tactics, techniques, and procedures used by threat agents to develop and execute cyberattacks

g) whitelisting

a strategy where only pre-approved entities are granted access

The Macquarie Dictionary definition applies where terms are not defined within the RISSB Glossary or above.

Contents

Appendix Contents

1 Introduction

1.1 Purpose

The primary aim of this white paper is to present and analyse the findings from the Railway Cyber Security Survey conducted by Griffith University in collaboration with the Rail Industry Safety Standards Board (RISSB). This survey seeks to evaluate the current state of cybersecurity maturity within the Australian railway industry. By examining the cybersecurity measures, practices, and challenges faced by rail organisations, this white paper aims to:

- Assess Industry Maturity: Provide a comprehensive overview of the railway industry's maturity in cybersecurity, highlighting strengths and areas for improvement.
- Inform Strategic Decisions: Offer insights to rail organisations that will inform strategic decisions and policymaking to enhance cybersecurity frameworks and resilience within the industry.
- Enhance Awareness: Raise awareness about the critical importance of cybersecurity in the railway sector, emphasising the potential risks and impacts of cyber-attacks on national infrastructure and public safety.
- Support Industry Collaboration: Foster collaboration and knowledge sharing among rail organisations, encouraging the adoption of best practices and collective efforts to mitigate cybersecurity risks.
- Guide Future Research: Identify gaps and opportunities for further research and development in railway cybersecurity, guiding future academic and industry initiatives to bolster cyber defences.

This white paper serves as a valuable resource for stakeholders within the railway industry, including policymakers, security professionals, and organisational leaders, to understand and enhance the cybersecurity posture of Australia's rail networks.

1.2 RISSB's role in advancing rail safety and standards

Introduction to RISSB and its role in the rail industry

RISSB collaborates closely with the rail sector to standardize safety procedures nationwide. Through its committees, groups, and forums, RISSB fosters networking and information exchange, promoting national harmonisation and interoperability. By advancing technical and operational consistency, RISSB enhances productivity, reduces costs, and improves safety Standards throughout the industry.

RISSB's contribution to rail industry Standards

RISSB provides essential resources to rail companies, including good practice Standards, codes of practice, guidelines, and rules. With over 250 published products, RISSB is Australia's only accredited Standards development agency for the rail industry. These publications support the industry in enhancing productivity, reducing costs, and enhancing safety measures. Additionally, RISSB extends its support to the rail industries in New Zealand, ensuring widespread access to its valuable materials.

The significance of cybersecurity in the rail industry

Cybersecurity holds paramount importance in the railway industry due to the integral role of technology in meeting commercial and operational demands. Cyber threats targeting computer-based railway systems pose serious risks, including potential loss of life, injuries to passengers and staff, operational disruptions, economic losses, reputational damage, and infrastructure damage. Various factors, including organizational interfaces, system interfaces, workforce activities, and third-party usage of technology, can instigate cyber threats, complicating the task of securing vast railway networks.

RISSB AS 7770 Rail Cyber Security Standard

Recognizing the critical nature of cybersecurity, RISSB developed the AS 7770 *Rail Cyber Security* Standard. This Standard, in conjunction with the *Rail Cyber Security Guideline*, defines the standards for managing cybersecurity risks within the Australian railway network. It focuses on preserving the reliability, availability, maintainability, and safety (RAMS) of rail control systems, as well as ensuring the confidentiality, integrity, and availability of data in auxiliary systems and the privacy of customer information.

Objectives of AS 7770 Standard

The primary objective of the AS 7770 Standard is to identify and address cyber-risks that could compromise the reliability, availability, maintainability, and safety of railway operations. Developed by industry experts, including digital systems engineers and security architects with extensive rail control systems and cybersecurity knowledge, AS 7770 is a comprehensive guide for RTOs, suppliers, subcontractors, and maintenance contractors. It equips personnel responsible for cybersecurity with the necessary information to effectively navigate evolving demands in the sector.

2 About the survey

2.1 Survey-based research overview

This survey-based research focuses on cybersecurity within the railway industry, specifically examining the cybersecurity controls implemented by railway organizations. The process began with preparing an information sheet, which was reviewed and approved by RISSB to ensure alignment with research objectives. Subsequently, RISSB distributed the information sheet to relevant RTOs or railway organizations, detailing the research purpose, known risks, expected benefits, confidentiality measures, and voluntary participation.

2.2 Survey distribution and participation

After receiving approval from RISSB, the survey was disseminated through the *RISSB Connect* weekly newsletter, which highlighted the collaboration with Griffith University and emphasized the significance of the research outcomes in enhancing rail cybersecurity vigilance and practices. Out of the 160 affiliated railway organizations, 42 actively participated in the research initiative, with 40 of these organizations focusing specifically on operational aspects of railway management.

2.3 Survey design and questionnaire

An outline of research questions was prepared before the final survey was sent. The survey comprised 42 questions, including yes/no, agree/disagree, multiple-choice, and linear scale questions. Designed using Google Forms for security and user privacy, it required participants to provide consent before commencement. Criteria for evaluating responses were established, with efficiency, moderate, and below-average ratings determined based on respondent choices for each question.

2.4 Data analysis and practices utilized

Survey results were analysed and represented using graphs and charts. Additionally, secondary sources such as articles, research papers, journals, and RISSB reports were reviewed. Throughout the research period, formal and informal discussions were held with RISSB. The survey questions were informed by AS 7770 *Rail Cyber Security*, which defines 154 practices across 18 controls. This Standard aligns with the NIST framework, renowned for developing benchmarks and best practices in critical infrastructure cybersecurity, influencing global cybersecurity Standards adoption.

Table 2-1 Practices for the Formation of Survey Questions

Controls	Capability
Access Control (AC)	• Determine the system's access needs • Limit access to internal systems • Manage system access remotely • Only allow authorized people and processes access to data
Contingency Planning (CP)	• Continuity plan or a disaster recovery plan • Ensure continuity of core services under cyber or physical attack • Testing includes low-probability high-impact cyber-physical attack scenarios
Audit & Accountability (AU)	• Establish auditing necessities • Conduct audits • Recognize and safeguard audit data • Examine and maintain audit logs
Awareness & Training (AT)	• Organize security awareness events • Organize training
Configuration Management (CM)	• Form baseline configurations • Organize and manage configurations and changes
Identification & Authentication (IA)	• Allow authenticated entities to gain access
Incident Response (IR)	• Prepare a response plan for an occurrence • Recognize and report on occurrences • Create and implement a plan of action in the event of a proclaimed emergency • Conduct post-incident investigations • Put incident response to the test
Maintenance (MA)	• Take care of routine maintenance
Media Protection (MP)	• Recognize and label media • Media protection and control • Cleanse the media • Transport media in a safe manner
Personnel Security (PS)	• Perform background checks on employees • Prevent CUI from being harmed by personnel whereabouts
Physical and Environment Protection (PE)	• Restriction of physical access
Protect (PR)	• Sufficient remote access capability to allow systems engineering and other support staff to work from home (or a remote office) in a disaster
Planning (PL)	• Documented security architecture and plan considered mandatory for critical infrastructure • Periodically updated plan to reflect change
Risk Assessment (RA)	• Vulnerability scanning, including of Industrial Control System (ICS) • Classify safety-critical and non-safety critical systems and networks
Security Assessment & Authorization (CA)	• Create and maintain a security plan for system • Controls must be defined and managed

Controls	Capability
	• Review the code
Situational Awareness (SA)	• Monitoring threat using surveillance systems
System & Communications Protection (SC)	• Establish security standards for systems and communications • Maintain communication control at the system's edge
System & Information Integrity (SI)	• Recognize and address problems in the information system • Recognize potentially harmful data/matter • Monitor the network and system • Set up enhanced email security

3 Survey Outcomes

3.1 Overview of cyber-compliance levels

Survey-based analysis of cyber-compliance levels in the railway industry

The survey results provide valuable insights into the cyber-compliance levels within the railway industry, categorized into five distinct levels of cyber-hygiene practices: Level 1 (basic), Level 2 (intermediate), Level 3 (good), Level 4 (proactive), and Level 5 (advanced/progressive).

Overall cyber-compliance

The overall cyber-compliance, calculated as a percentage, revealed the following observations:

Level 1 (Basic Cyber Hygiene): 34.45% of the railway industry demonstrated compliance with basic cyber-hygiene practices, emphasizing foundational security measures.

Level 2 (Intermediate Cyber Hygiene): Surpassing Level 3, 38.1% of the industry exhibited compliance with intermediate practices, indicating a stronger focus on documentation processes over management protocols.

Level 3 (Good Cyber Hygiene): 30.79% of railway organizations adhered to good cyber-hygiene practices, showcasing a slightly lower implementation rate compared to Level 2.

Level 4 (Proactive Cyber Hygiene): Notably, 33.84% of railway entities demonstrated compliance with proactive practices, emphasizing the importance of reviewing adherence to implemented procedures.

At Level 5 (Advanced/Progressive Cyber Hygiene), survey results revealed the lowest compliance, with only 27.56% efficiency, indicating a significant gap in optimizing cybersecurity practices.

Implications and Conclusions

Documentation vs. Management: The higher compliance rates in Level 2 suggest a stronger emphasis on documentation processes compared to management practices within railway organizations.

Reviewing vs. Optimizing Practices: While there are sufficient processes for reviewing adherence to implemented practices (Level 4), optimization of practices (Level 5) remains a challenge, as evidenced by the lower compliance rate.

These findings underscore the importance of enhancing cybersecurity measures within the railway industry, particularly in optimizing practices to achieve advanced cyber-hygiene standards. Addressing these gaps will be essential for bolstering cyber-resilience and mitigating potential cyber threats effectively.

3.2 Analysis of cybersecurity practices in the rail industry

In relation to cybersecurity practices within the rail sector, several noteworthy observations have emerged from the responses provided by industry stakeholders.

1 – Configuration maintenance and security standards

Organizations effectively maintaining configurations and inventories tend to align more closely with established information security standards for continuity, redundancy, and availability. Conversely, those neglecting scans for unauthorized ports often resort to periodic penetration tests or prioritize the integrity of sensitive information (see Figure 1 in Appendix A).

2 – Awareness training and insider threat monitoring

Organizations showing a strong disagreement regarding providing awareness training to recognize and report insider threats exhibit a low tendency to monitor personnel and system components for suspicious activity. This indicates a potential deficiency in implementing a robust cybersecurity framework (see Figure 6).

3 – Encryption and detection of cyber-crime events

Organizations neglecting encrypted sessions for network device handling and failing to update mechanisms against malicious code demonstrate a diminished ability to detect cyber-crime events. Increased focus on basic cyber-hygiene practices, such as updating protective mechanisms, may compromise the effective implementation of intermediate cyber-hygiene (see Figure 7).

4 – Designated railway officials and cyber-hygiene practices

Organizations with designated railway officials for sanitizing or destroying information system media containing sensitive information tend to implement intermediate cyber-hygiene practices more effectively. This indicates moderate to good implementation of cyber-hygiene practices, including encrypting Controlled Unclassified Information (CUI) on mobile devices (see Figure 8).

5 – Blacklisting, whitelisting, and screening individuals

Effective implementation of blacklisting and whitelisting policies, coupled with strong awareness among systems administrators regarding security risks, leads to robust screening of individuals accessing CUI. Conversely, organizations lacking these policies and managerial awareness demonstrate poor screening practices (see Figure 9).

6 – Response to anomalous activities

Organizations exhibit a linear increase in their ability to respond to suspicious activities and critical indicators as assets are monitored and logs are recorded more effectively (see Figure 10).

7 – Monitoring boundary communications and cyber-hygiene practices

A direct correlation exists between implementing good cyber-hygiene practices, such as data backups and scanning for malicious code, and the effectiveness of proactive cyber-hygiene practices. An inverse relationship exists between monitoring boundary communications and proactive cyber-hygiene, indicating the need for a balanced approach (see Figure 13).

8 – Operations centre and security solutions evaluation

A linear relationship exists between the presence of an operations centre and the frequency of evaluating and improving security solutions. However, an efficient implementation of proactive cyber-hygiene practices may only lead to a moderate implementation of advanced cyber-hygiene practices (see Figure 16).

9 – Audit logs and physical access restrictions

Effective examination of audit logs for physical access correlates with stricter restrictions on access to information systems. Implementation of boundary communication monitoring influences an organization's ability to monitor security controls and develop risk assessment/mitigation plans (see Figure 17).

Overall, the analysis underscores the importance of robust cybersecurity practices within the rail industry to mitigate cyber threats effectively and ensure the security of critical infrastructure. (See corresponding figures for detailed insights.)

4 Recommendations

The survey results indicate that while most sectors within the railway industry (i.e. more than 67%) report moderate to efficient levels of compliance with basic and intermediate cyber-hygiene practices, the overall implementation of good cyber-hygiene practices remains moderate to below average. Notably, most railway organizations report below-average compliance with proactive and advanced cyber-hygiene practices. These findings underscore the imperative for railways to adopt a more proactive stance towards cybersecurity to mitigate unforeseen cyber-threat situations (see Figure 1 in Appendix A).

1 – Foster continuous improvement and systematic evaluation of cybersecurity practices

Organizations should strive for cohesion in reviewing and optimizing their practices and procedures for safeguarding against malicious cyber threats. It is crucial to document and review and actively optimize security practices and procedures to enhance their efficacy. Cultivating a culture of continuous improvement and innovation in cybersecurity measures will enable organizations to avoid potential risks. Establishing a systematic and periodic evaluation of security measures ensures their effectiveness against evolving cyber threats. Furthermore, implementing a feedback mechanism for employees to provide insights on potential optimizations fosters a collaborative and adaptive approach. For a detailed visualization of these findings, see Figure 4.

2 – Establish cross-functional collaboration for improved authentication and incident documentation

To enhance authentication and incident documentation practices within organizations and consequently improve the effectiveness of reviewing cyber threats influencing the risk context, it is recommended to establish cross-functional collaboration between IT, security teams, and other relevant departments. This approach facilitates a holistic incident response strategy. Encouraging a culture of transparency and accountability in incident reporting is vital to understand the threat landscape thoroughly. For a detailed visualization of these findings please see Figure 5.

3 – Maintain up-to-date cybersecurity training and post-incident analysis

Organizations should ensure their cybersecurity training materials remain current to reflect the evolving threat landscape. Following a cyber incident, conducting a thorough post-incident analysis and utilizing it as a learning opportunity to identify areas for improvement is recommended. The RISSB AS 7770 *Rail Cyber Security*, code of practice, and *Rail Cybersecurity Guideline* emphasize the crucial role of adequate funding in implementing effective cybersecurity training, facilitating the development of sophisticated training modules, realistic simulation exercises, and up-to-date resources. For a comprehensive visual representation of these findings, see Figure 6 and Figure 11.

4 – Implement RISSB Standard AS 7770 for network security and proactive cybersecurity culture

Organizations are recommended to leverage the RISSB AS 7770 Standard, to implement robust network perimeter security measures. Additionally, fostering a proactive cybersecurity culture by implementing

encryption protocols for sensitive data transmission and establishing clear policies for secure information exchange across organizational boundaries is crucial. Emphasis should be placed on regular software updates, encryption protocols, and robust third-party risk management practices as outlined in the Standard. Implementing practices such as network security measures, policy reviews, collaboration with cybersecurity experts, and continuous monitoring informed by threat intelligence can collectively result in a resilient and secure cyber-environment for railway organizations. Figure 8 and Figure 16 provide a detailed visualization of these findings.

5 References

National Institute of Standards and Technology. “NIST Cybersecurity Framework for Improving Critical Infrastructure Security Version 1.1.” April 16, 2018.

RISSB. “Australian Rail Network Cyber Security Strategy.” 2018. Retrieved February 12, 2023, from https://www.rissb.com.au

Stewart, C., and Hall, K. a. H. "An Introduction to the Cybersecurity Maturity Model Certification (CMMC)." 2020. Retrieved November 20, 2021, from <https://insights.sei.cmu.edu/blog/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc/>

Jones, R., and Broz, K. W. "Cybersecurity: How to Successfully Navigate CMMC & the DFARS." 2020.

RISSB. “Rail Cyber Security for Rolling Stock & Train Control Systems – Code of Practice.” 2020. Retrieved February 12, 2023, from https://www.rissb.com.au

National Institute of Standards and Technology. “Guide for Conducting Risk Assessments, NIST SP800-30 Revision 1.

National Institute of Standards and Technology. “Guide to Industrial Control Systems (ICS) Security, NIST SP800-82 Revision 2.

National Institute of Standards and Technology. “Security and Privacy Controls for Federal Information Systems and Organizations, NIST SB 800-53 rev 4.

RISSB. “Rail Cyber Security Implementation of AS 7770:2018 Guideline.” 2018. Retrieved February 12, 2023, from https://www.rissb.com.au

Center for Internet Security. “The CIS Critical Security Controls for Effective Cyber Defense.”

Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts, ISO/IEC TR 15443-1:2012.

Appendix A Analysis estimating the mean of one cybersecurity factor with respect to two other categorical cybersecurity factors

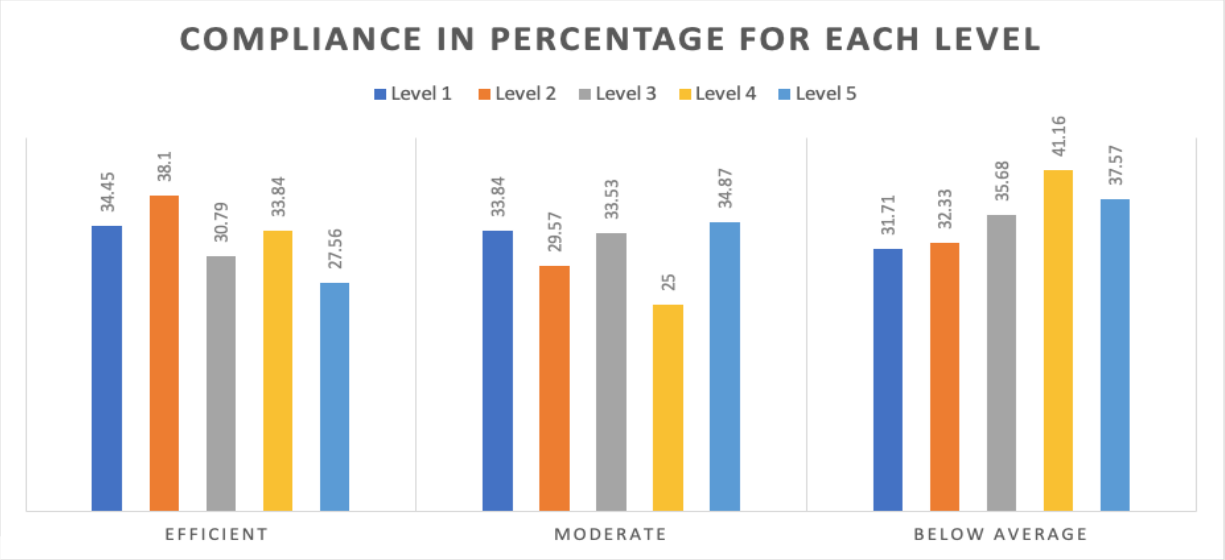


Figure 1 Railways cybersecurity overall compliance

The overall compliance has been discussed in detail in the executive summary and analysis section of the report.

Analysis of organizational awareness and compliance of baseline configurations and URL filtering

Q11. To what extent are baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) established and maintained?

Q30. Your organization uses procedures to enforce URL filtering of unapproved websites?

Q37. How well does your organization ensure that information processing facilities fulfill organizationally established information security standards for continuity, redundancy, and availability?

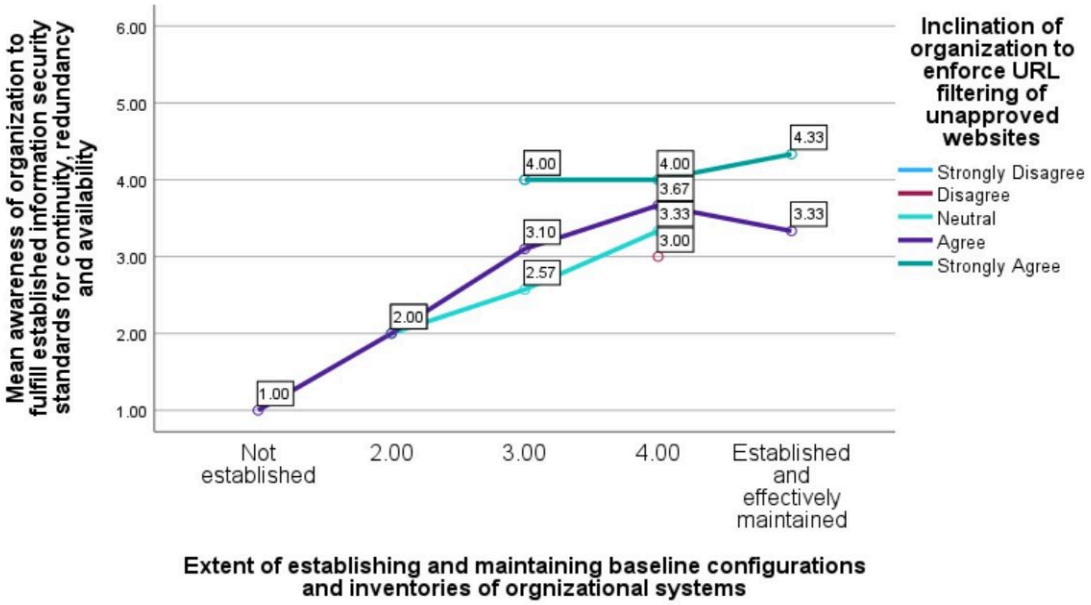


Figure 2 Organizational awareness of information security standards of baseline configurations and URL filtering

Figure 2 shows a clear relationship among Level 2, Level 4, and Level 5.

Officials who strongly support URL filtering and maintain moderate baseline configurations exhibit a mean value of 4, indicating compliance with organizationally established information security standards. Conversely, officials who disagree with URL filtering and only adopt baseline configurations rated as "good" (4) have a mean value of 3 for meeting these standards.

An observation reveals that officials reporting effective maintenance of configurations and inventories also demonstrate a high estimated marginal mean concerning facilities meeting organizationally established information security standards, particularly regarding continuity, redundancy, and availability.

To assess organizational compliance with configuration management, attention is primarily directed towards implementing practices CM8, CM2, and CM6, as indicated on the x-axis of the graph.

Similarly, evaluating compliance with network security practices pertaining to system and communication protection involves creating separate lines, as depicted on the right side of the graph.

Furthermore, understanding compliance with physical and environmental protection, as well as contingency planning, centres on implementing practices PE9-16 and CP1, CP2. These practices are pivotal in evaluating the estimated marginal mean along the y-axis of the graph.

Analysis of organizational awareness and compliance in penetration testing and cybersecurity practices

Q31. How well do you rate your organization in conducting periodic penetration tests and designing network system security capabilities to review indicators of compromise?

Q29. Does your organization perform scans for unauthorized ports available across network boundaries, over the organization's Internet network boundaries and other organizationally defined boundaries?

Q24. Which of the following measures are used by your organization to protect organizational communication and preserve the integrity of sensitive information?

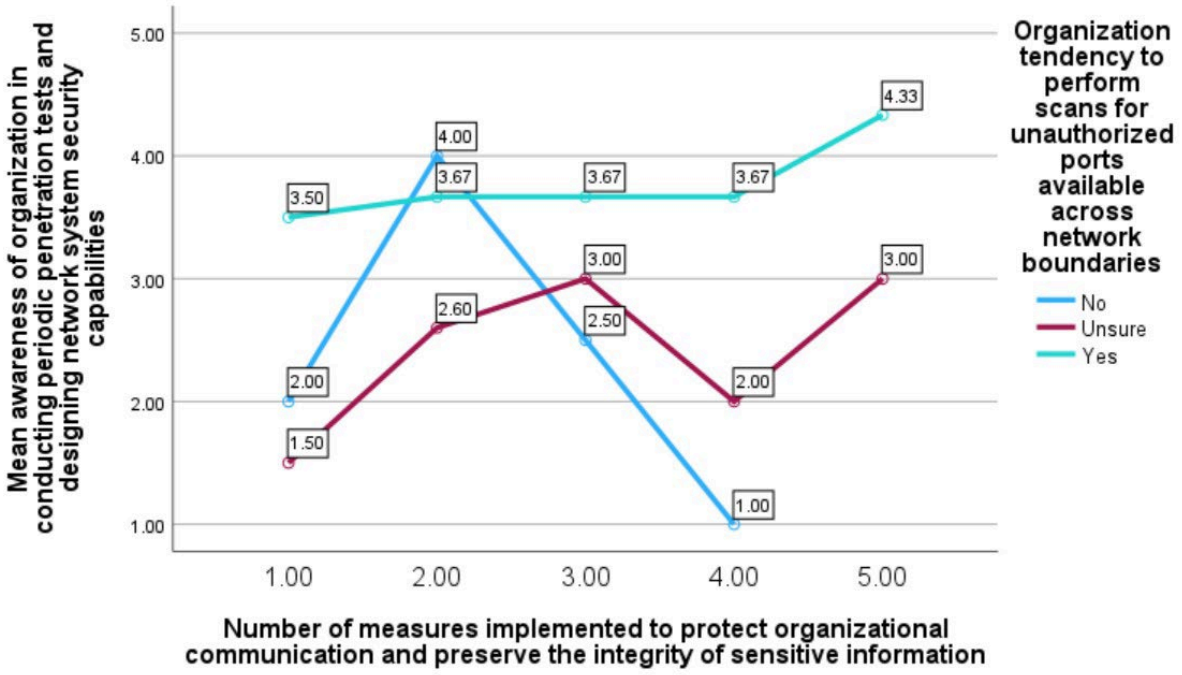


Figure 3 Organizational awareness of penetration testing of unauthorized port scans and organizational communication protection

When officials opt out of performing scans and instead adhere to efficient (4) measures, the minimum mean for conducting penetration testing is 1. Conversely, those who adhere to minimum to low measures (2) have a marginal mean value of 4 for conducting penetration testing. This indicates that when respondents answer 'no' to performing scans for unauthorized ports, they effectively practice either periodic penetration testing or prioritize preserving the integrity of sensitive information.

Officials who select "unsure" as an option regarding performing scans and follow measures ranging from least to moderate (1-3) exhibit a trend similar to officials answering "yes." Conversely, officials opting for efficient (4) measures show a trend similar to those choosing 'no' as a response. This suggests that officials who are uncertain about performing scans for unauthorized ports indicate a trend that is a mix of responses 'yes' and 'no.'

To assess organizational compliance with incident response, particular emphasis is placed on the implementation of practices IR3 and IR8, which were pivotal for evaluating the estimated marginal mean along the y-axis of the graph. Additionally, attention is directed towards periodic testing and assurance cycles that align with cybersecurity goals, risk assessments, and the cadence of governance arrangements and iterative/programmatic milestones.

Moreover, to gauge compliance with contingency planning, configuration management, and system & communications protection practices, namely CP4, CM7, and SC7, respectively, separate lines are delineated on the right side of the graph.

Furthermore, to ascertain compliance with System and Information Integrity, Access Control, Physical and Environmental Protection, and Planning, the focus predominantly rests on the implementation of practices SI8, SI3, AC4, PE4, PL1, PL2, and PL8. These practices are integral factors along the x-axis of the graph.

Assessment of organizational risk management, security policies, and wireless network security practices

Q16. Which of the following practices that manage risks and assess overall security of organizational systems are followed by your organization?

Q27. Is there an application vetting procedure that allows only those applications which conform to the organization's security policy to be used?

Q33. How often does your organization identify and mitigate risks associated with unidentified wireless access points connected to the network?

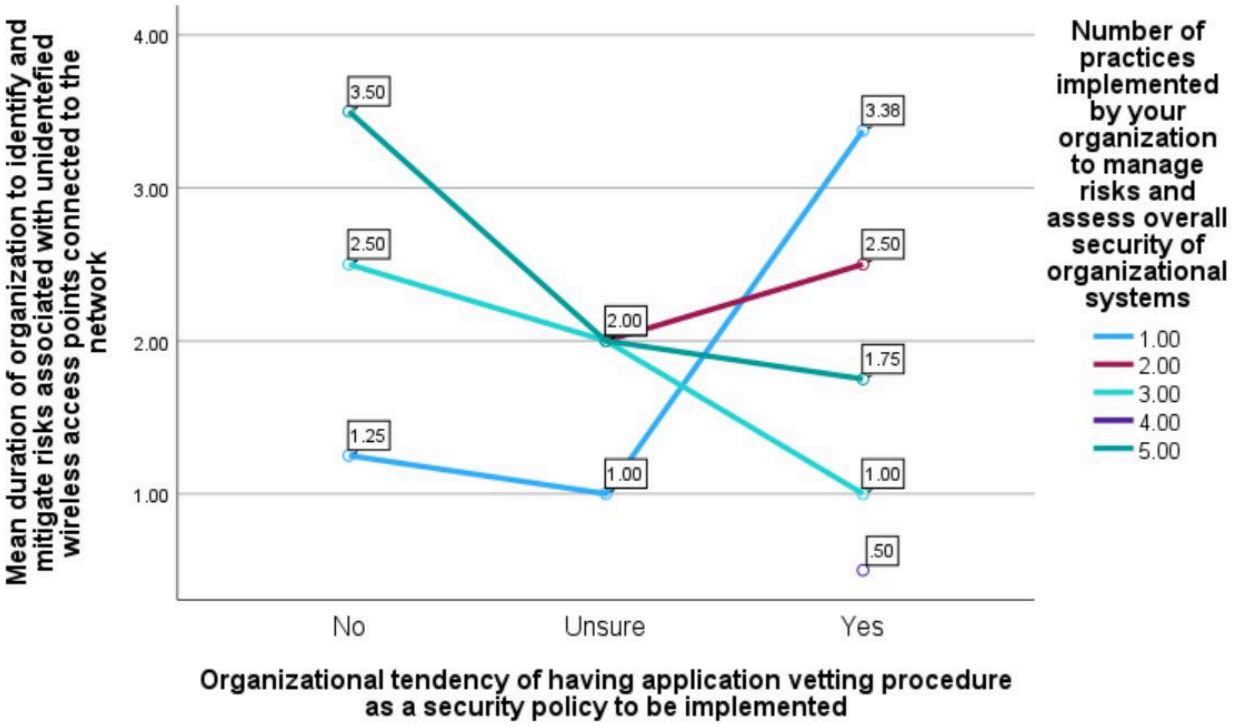


Figure 4 Mean organizational awareness of identifying and mitigating risks within the context of having application vetting procedures and overall security assessment of organizational systems

For organizations that select only one practice and neglect the application vetting procedure, the mean value for identifying and mitigating risks associated with unidentified wireless access points connected to the network is 1.25. Conversely, those opting for "yes" experience an increased mean of 3.38.

On the other hand, organizations selecting all 5 options and implementing the application vetting procedure as a security policy ("yes" option) fail to identify and mitigate risks associated with unidentified wireless access points. This indicates that the adoption of practices at levels 2 and 4 does not guarantee the adoption of level 5 practices.

In essence, organizations that document (level 2) and review (level 4) their practices and procedures might not necessarily optimize (level 5) them for mitigating cyber threats. This suggests a disparity between documenting and reviewing practices and the optimization required for safeguarding against cyber threats.

Moreover, organizations choosing all 5 parameters to manage risks and assess overall security but selecting "no" for having an application vetting procedure as a security policy have a mean frequency of 3.50 for identifying and mitigating risks associated with unidentified wireless access points. This implies that while these organizations document and optimize their practices, they are not inclined towards reviewing their security protocols. Additionally, they tend to mitigate risks without reviewing the procedures and practices.

To assess organizational compliance with Risk Assessment, practices RA5 and RA1 are considered, creating separate lines on the right side of the graph. Similarly, to understand compliance with Identification & Authentication and System & Information Integrity, practices IA4, IA5, and SI4 are focused on, aligning with the x-axis of the graph.

To assess organizational compliance with Access Control, particular attention is placed on the implementation of practices AC18 and AC17, which are crucial factors for evaluating the estimated marginal mean along the y-axis of the graph.

Furthermore, the evaluation extends to various wireless communication technologies utilized, including train radio, commercial mobile phone and/or cellular communication networks, satellite communications, and Wi-Fi networks. These technologies play a significant role in understanding the landscape of communication infrastructure within the railway system and its associated cybersecurity measures.

Analysis of organizational awareness in threat review, incident reporting, and authentication practices for RTOs

Q2 Are there proper authentication measures setup to verify identities of users or devices which are granted access to your organization's information systems?

Q20. To what extent does your organization track, document and report malicious incidents to designated officials in case of cyber threat?

Q21.Your organization regularly reviews the threat context to detect and highlight any emerging trends that may influence the risk context in which the RTO (Rail Transport Operator) operates.

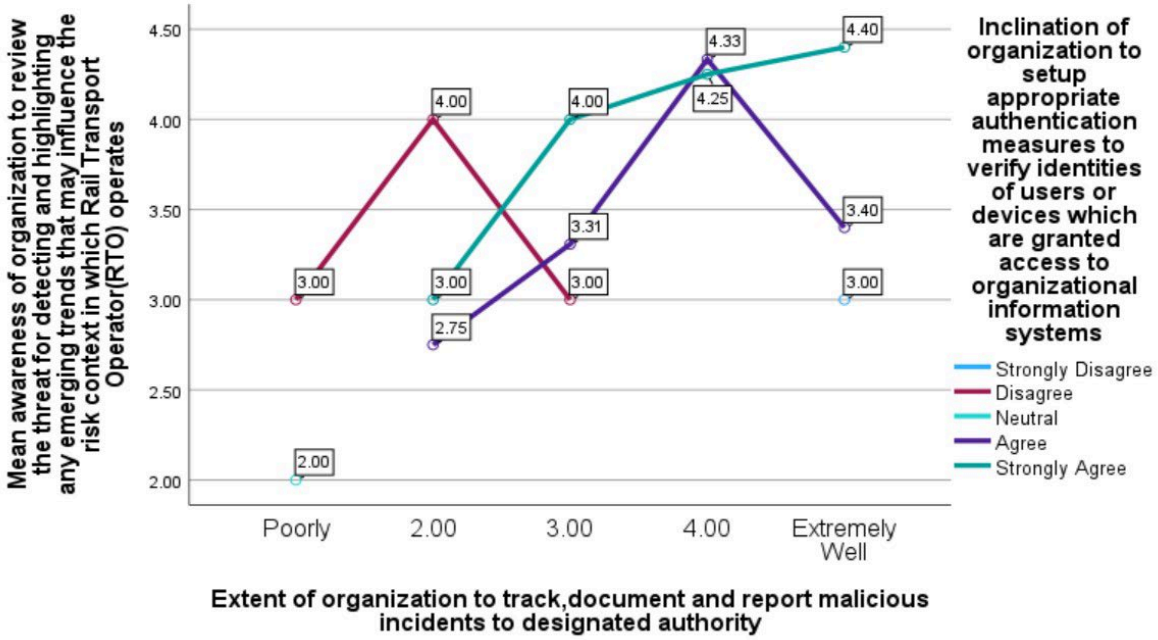


Figure 5 Mean organizational awareness to review threats influencing RTO within the context of reporting malicious incidents and user identity verification

For organizations whose officials strongly advocate for setting up proper authentication measures, there's an evident increasing trend for Level 3 practice, specifically in reviewing threats to detect and highlight emerging trends that may influence the risk context in which the Railway Traffic Operations (RTO) operates. This trend coincides with another Level 3 practice of tracking, documenting, and reporting malicious incidents to designated officials in the event of a cyber threat.

Those organizations whose officials strongly support setting up proper authentication measures and excel in tracking, documenting, and reporting malicious incidents exhibit the highest marginal mean value of 4.40 for regularly reviewing the threat context.

Conversely, organizations where officials moderately agree to setting up proper authentication measures and perform poorly in tracking, documenting, and reporting malicious incidents show the lowest estimated marginal mean of 2 for reviewing threats. However, if these organizations strongly disagree with setting up proper authentication measures but effectively track, document, and report malicious incidents, their estimated marginal mean is moderate (3).

It's notable that when both practices are diligently followed, high marginal means are observed. Conversely, implementing only one practice results in moderate marginal means. Organizations exhibiting moderate to below-average implementation of both practices yield poor marginal means.

To assess organizational compliance with Access Control, practice AC4 is examined, creating separate lines on the right side of the graph.

Additionally, to gauge compliance with Incident Response, practices IR4 and IR6 are focused on, aligning with the x-axis of the graph.

Furthermore, understanding compliance with Risk Assessment and Planning involves implementing a systematic approach to identifying and evaluating risks, documenting assets for defence, and implementing safety and security risk management plans for rail control systems. These factors contribute to the evaluation of the estimated marginal mean along the y-axis of the graph. Emphasis is placed on the risk management system containing procedures for reviewing risk plans annually, considering changes to internal or external conditions, and conducting threat analysis and control assessments by qualified and competent personnel.

Evaluation of organizational adherence to cybersecurity frameworks in projects: impact of awareness training and monitoring practices

Q19. Awareness training is provided to recognize and report insider threats, as well as to communicate cyber threat intelligence to the authorized personnel and the stakeholders.

Q40. How thoroughly does your organization monitor personnel and system components for suspicious activity?

Q42. To what extent does your organization require that all projects include a cybersecurity framework?

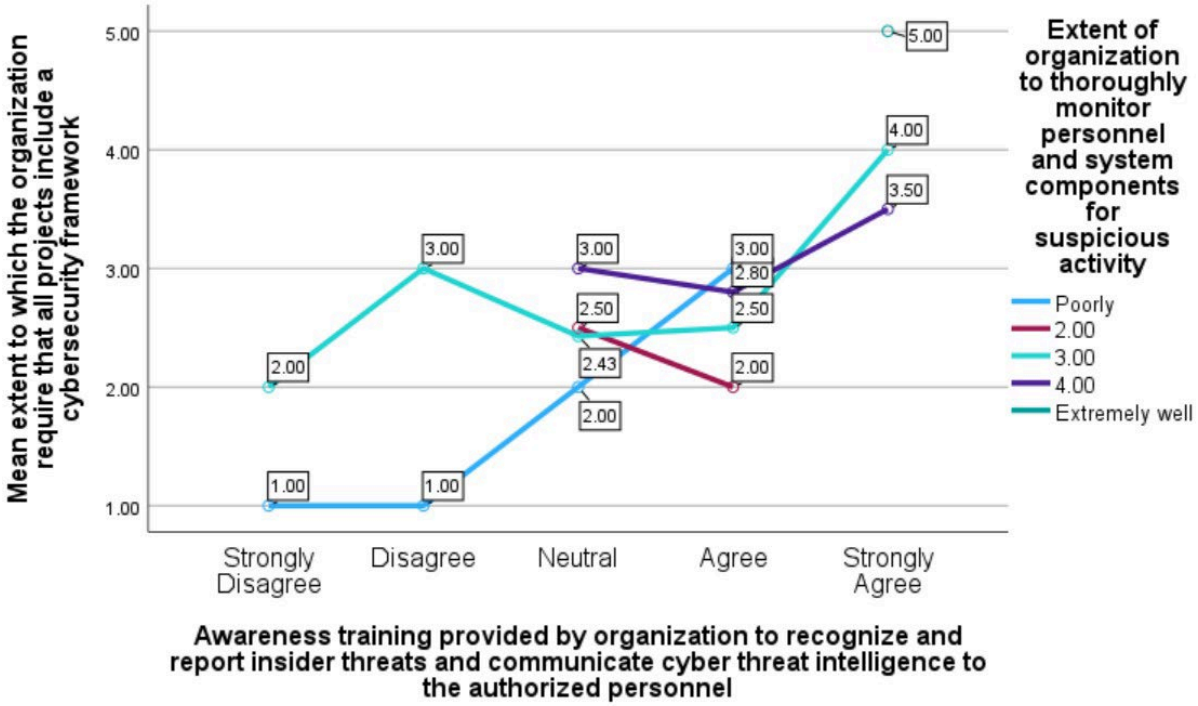


Figure 6 Mean organizational awareness of projects including cybersecurity framework within the context of awareness training and monitoring of personnel, system components

Organizations that strongly advocate for awareness training to recognize and report insider threats, coupled with thorough monitoring of personnel and system components for suspicious activity, estimate that their projects require a cybersecurity framework, with an estimated marginal mean of 5 (maximum). Conversely, those who strongly disagree with providing awareness training for insider threats and exhibit minimal tendency to monitor personnel and system components for suspicious activity have an estimated marginal mean of 1, indicating a low tendency to incorporate cybersecurity frameworks in their projects.

Furthermore, organizations that moderately adhere to both practices have a mean of 2.43 for including cybersecurity frameworks in their projects.

To assess organizational compliance with Incident Response, Planning, Awareness & Training, and Contingency Planning, practices IR2, IR7, PL4, AT2, AT3, AT1, CP2, and CP3 are focused on, aligning with the x-axis of the graph.

Moreover, to understand compliance with System & Information Integrity, Physical & Environmental Protection, and Personnel Security, practices SI4, PE3, PE6, and PS respectively are examined, creating separate lines on the right side of the graph.

Additionally, the Railway Traffic Operations (RTO) should have a security management system addressing the five functions of the RISSB Cybersecurity Framework, developed utilizing NIST protocols: identify, protect, detect, respond, and recover. These factors contribute to the evaluation of the estimated marginal mean along the y-axis of the graph.

Analysing organizational effectiveness in cyber-crime detection and reporting: influence of mechanism updates and encrypted sessions

Q7. How often are mechanisms (which protect organizational information against malicious code) updated?

Q12. Does your organization use encrypted sessions to handle network devices and permit cryptographically secured passwords?

Q13. How well does your organization detect cyber-crime events, report cyber-crime events, and perform maintenance on organizational systems after such events?

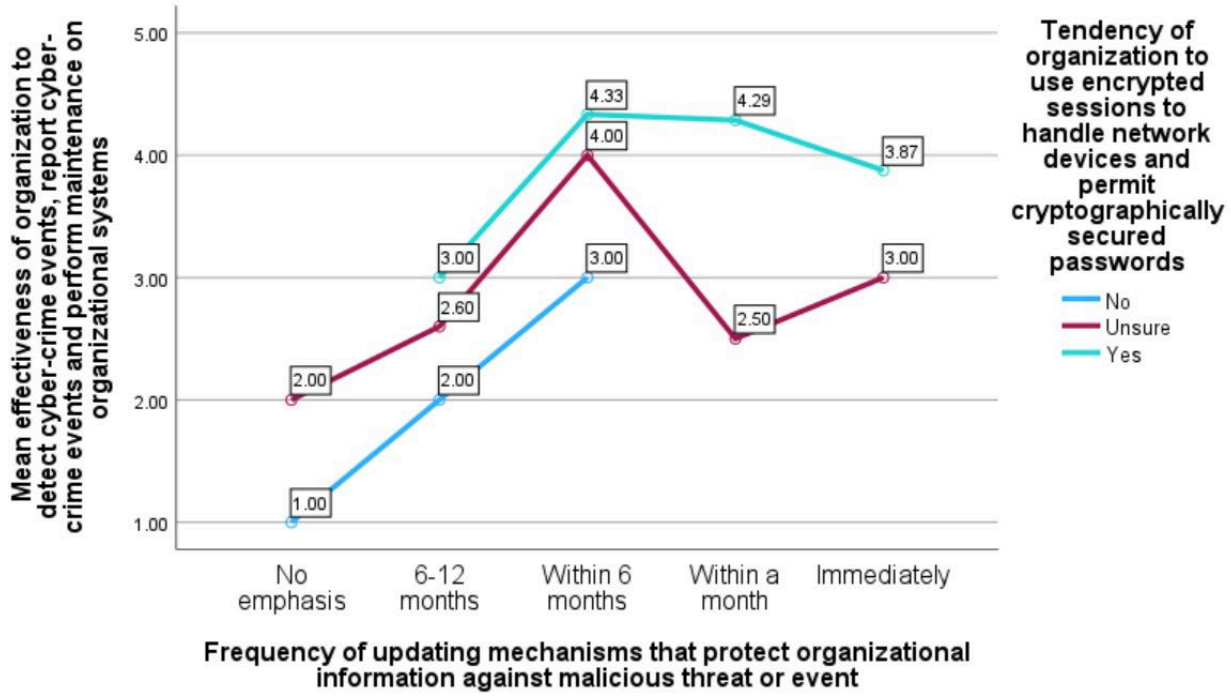


Figure 7 Mean organizational effectiveness to detect and report cyber-crime events within the context of updating mechanisms and using encrypted sessions

For organizations opting not to use encrypted sessions to handle network devices and not emphasizing updating mechanisms against malicious code, there's a notable low tendency to detect cyber-crime events, with a marginal mean of 1.

Responses across all respondents, whether they chose 'yes,' 'no,' or 'unsure' for encrypted sessions to handle network devices and permit cryptographically secured passwords, indicate that the maximum marginal mean for detecting, reporting, and performing maintenance occurs at a moderate frequency (every 6 months) of updating mechanisms, with mean values of 4.33, 3, and 4, respectively.

However, as organizations focus more on increasing this frequency, i.e., emphasizing the level 1 practice of updating mechanisms to protect organizational information against malicious threats or events, the marginal means for the level 2 practice of the organization's effectiveness to detect cyber-crime events, report cyber-crime events, and perform maintenance on organizational systems after such events decrease. This indicates a compromise on the effective implementation of level 2.

To assess organizational compliance with System & Information Integrity, the focus primarily rests on the implementation of practice SI3, which is considered for the factor along the x-axis of the graph.

Furthermore, to understand compliance with System & Communications Protection, practices SC39, SC8, and SC12-13 are examined, creating separate lines on the right side of the graph. Additionally, Access Control practice AC6, which stipulates that devices accessing services should be treated as untrustworthy unless authenticated, with authentication ideally being cryptographic, is considered.

Moreover, to gauge compliance with Maintenance, the primary focus is on the implementation of practice MA6, contributing to the evaluation of the estimated marginal mean along the y-axis of the graph.

Evaluation of organizational practices in protecting Controlled Unclassified Information (CUI): impact of encryption, handling procedures, and media sanitization

Q17. How well does your organization encrypt CUI on mobile devices and define procedures for handling the CUI data?

Q9. How effectively is CUI being protected and controlled in compliance with the approved authorizations?

Q3 Does your organization have a designated railway official to sanitize or destroy information system media containing Federal Contract Information (FCI), before discarding or releasing it for reuse?

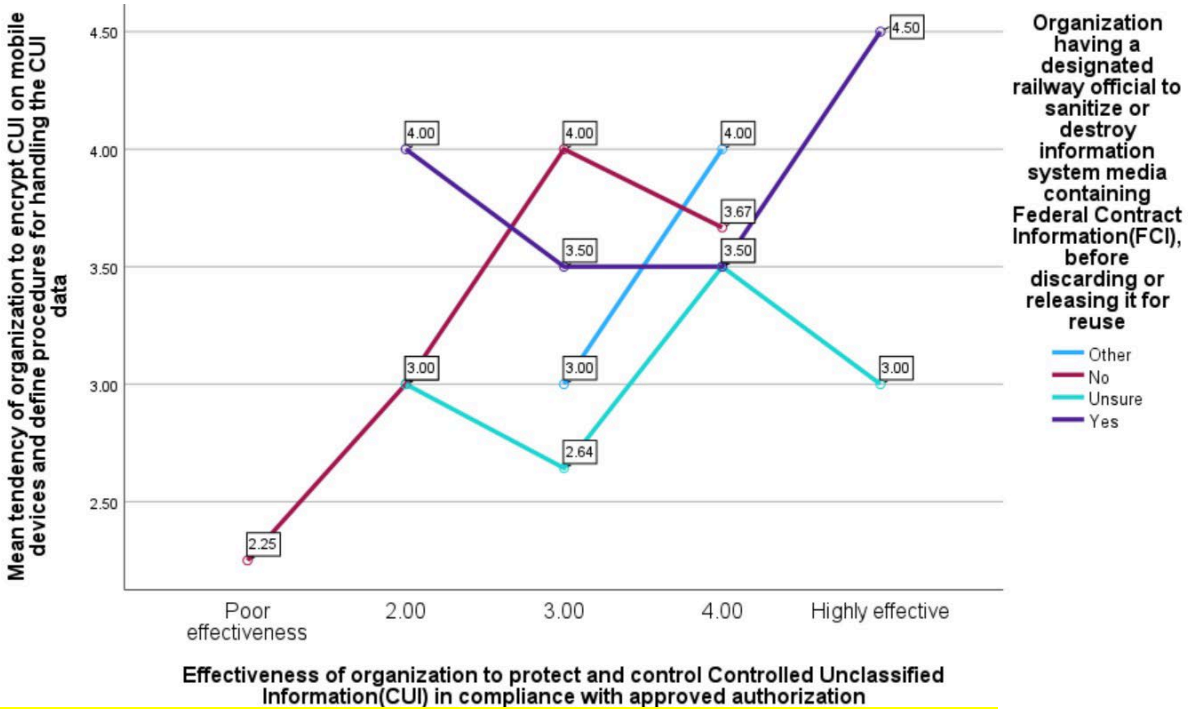


Figure 8 Organizational awareness to encrypt CUI data for protecting and controlling CUI and sanitizing or destroying media containing FCI

Organizations that effectively protect and control CUI and affirmatively choose to have a designated railway official to sanitize or destroy information system media containing Federal Contract Information (FCI) before discarding or releasing it for reuse demonstrate an estimated marginal mean of 4.5 for encrypting and handling CUI.

Conversely, organizations that opt not to have a designated railway official to sanitize or destroy information system media containing FCI exhibit a maximum marginal mean value of 4 when they moderately protect and control CUI.

These organizations, regardless of whether they answer 'yes' or 'no' to having a designated railway official for media sanitization, implement level 2 practices effectively to protect and control CUI in compliance with approved authorization, to a moderate to maximum extent. This also indicates a moderate to good implementation of level 3 practices, specifically the tendency of organizations to encrypt CUI on mobile devices and define procedures for handling CUI data.

To assess organizational compliance with System & Communications Protection and Identification and Authentication, the focus is on the implementation of practices SC12, SC13, and IA1, contributing to the evaluation of the estimated marginal mean along the y-axis of the graph.

Furthermore, to understand compliance with Physical & Environmental Protection, practices PE 9-16 are examined, creating factors along the x-axis of the graph.

Moreover, compliance with Access Control, specifically practice AC5, is assessed, creating separate lines on the right side of the graph.

Assessment of organizational practices in screening individuals for access to Controlled Unclassified Information (CUI): impact of security awareness and blacklisting/whitelisting policies

Q10. System administrators, users of organizational systems and managers are aware of security risks associated with the system audit logs, policies, standards and procedures in relation to cyber-hygiene.

Q14. How would you rate your organization in screening individuals before authorizing them to access the organizational systems that hold the CUI?

Q18. Do you agree that your organization periodically reviews, and updates logged events, making sure that Blacklisting and Whitelisting policies are followed?

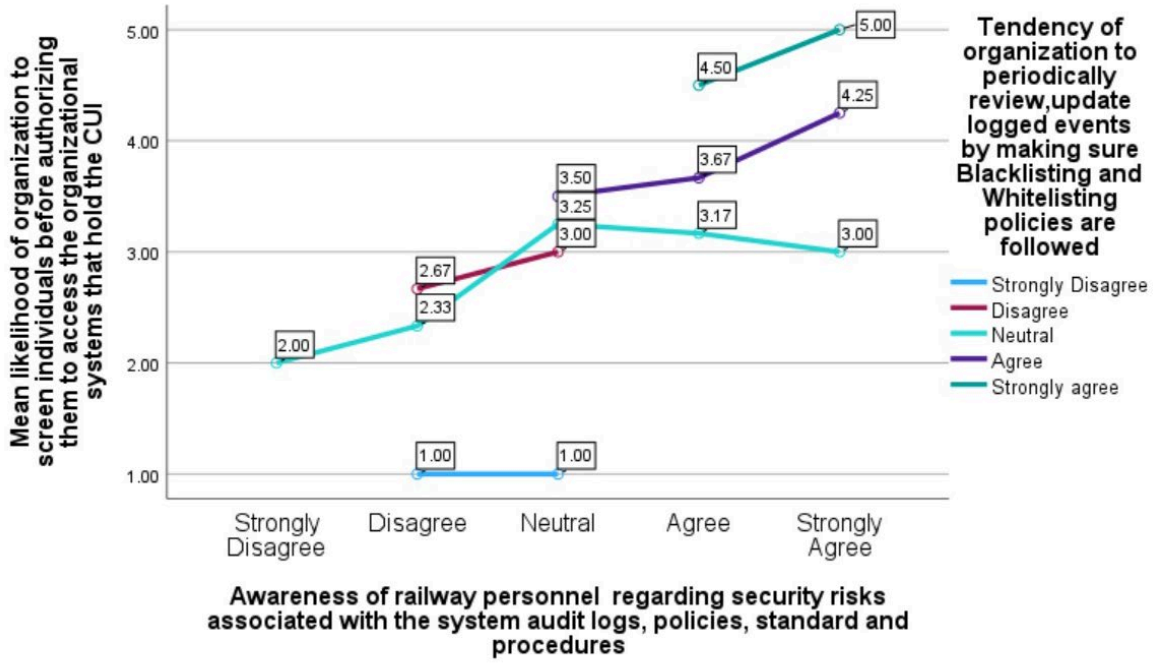


Figure 9 Mean organizational likelihood of screening individuals within the context of blacklisting and whitelisting policies and railway personnel awareness

Organizations efficiently following blacklisting and whitelisting policies and strongly agreeing that systems administrators are aware of security risks demonstrate a maximum mean marginal value of 5 for screening individuals before authorizing them to access CUI.

Conversely, organizations strongly disagreeing with having whitelisting and blacklisting policies and whose managers are only moderately aware of security risks indicate poor screening practices, with mean values of 1 for individuals accessing CUI.

Additionally, the estimated marginal mean values for screening individuals are higher when organizations perform periodic reviews, update logged events, and establish blacklisting and whitelisting policies more effectively.

To assess organizational compliance with Audit and Accountability and Security Assessment & Authorization, the focus is on the implementation of practices AU9 and CA1, contributing to the evaluation of the estimated marginal mean along the x-axis of the graph.

Furthermore, compliance with Personnel Security is assessed, focusing on the implementation of practices PS1-8, which contribute to the evaluation of the estimated marginal mean along the y-axis of the graph.

Moreover, compliance with System & Communications Protection, System & Information Integrity, Access Control, Configuration Management, and Identification & Authentication is evaluated through the implementation of practices SC7, SI3, SI4, AC4, AC20, CM7, and IA3, creating separate factors on the right side of the graph.

Assessment of organizational response to suspicious activities: influence of real-time responses, asset monitoring, and log recording

Q36. Which of the following types of real time responses are given by your organization to handle anomalous activities relating to incident patterns?

Q34. Your organization monitors assets and determines whether logs are recorded correctly.

Q26. To what extent does your organization review automated audit logs to detect and respond to suspicious activities (critical indicators like TTPs)?

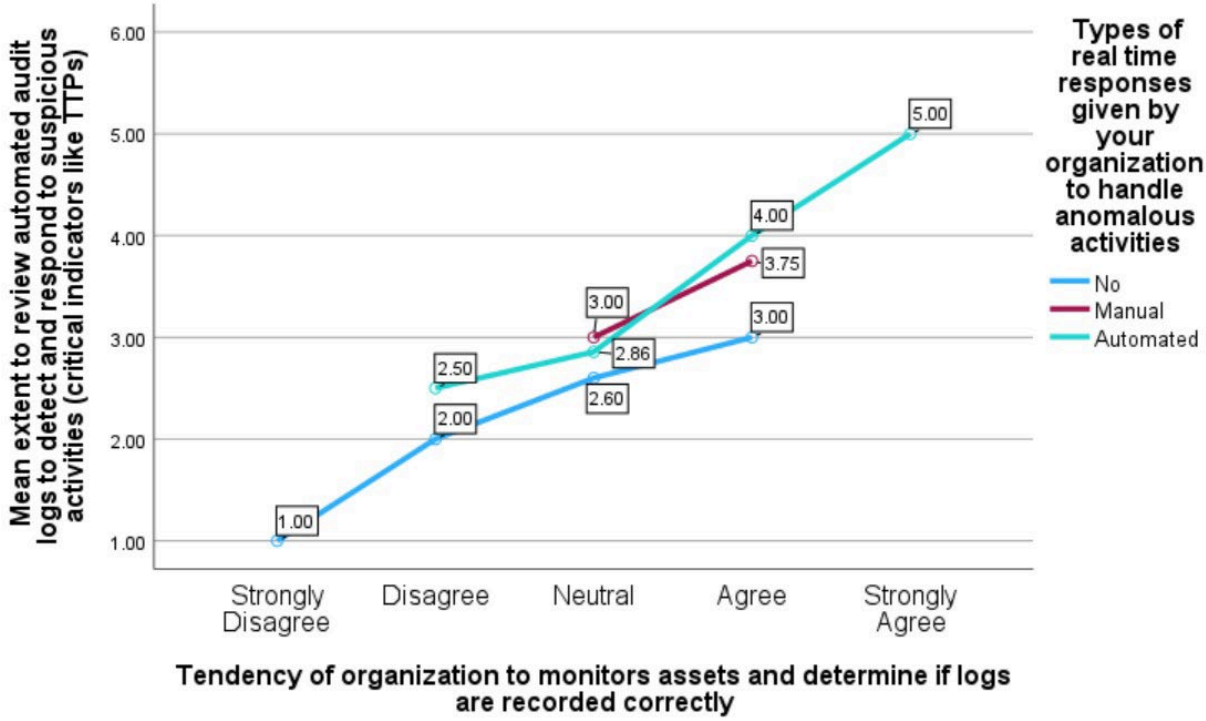


Figure 10 Mean organizational awareness to review automated audit logs within the context of real time responses and asset monitoring

Organizations that have automated real-time responses to handle anomalous activities and strongly agree to recording logs and monitoring assets effectively demonstrate a very high marginal mean value of 5 for detecting and responding to suspicious activities. Conversely, those with manual responses to handle anomalous activities and moderately to mildly effective recording logs and asset monitoring exhibit a moderate to good response to suspicious activities, with a maximum mean of 3.75.

For organizations selecting 'no' for real-time responses and strongly disagreeing with recording logs and monitoring assets, the means indicate a poor response mechanism to suspicious activities, with an estimated marginal mean value of 1.

Across all types of real-time responses given by organizations to handle anomalous activities (automated/manual/no response), there is a linear increase in the estimated marginal means of the organization to respond to suspicious activities and critical indicators like Tactics, Techniques, and Procedures (TTPs) as assets are monitored and logs are recorded more effectively.

To assess organizational compliance with Incident Response and System & Information Integrity, the focus lies on the implementation of practices IR6 and SI5, creating separate factors on the right side of the graph.

Furthermore, compliance with Contingency Planning, System and Communications Protection, and Audit & Accountability is evaluated through the implementation of practices CP6, SC28, and AU8, contributing to the evaluation of the estimated marginal mean along the x-axis of the graph. Additionally, monitoring level crossings helps meet safety regulations and improve maintenance procedures.

Moreover, measures implemented to enable the analysis of tools utilized by hackers and analysis of monitoring, logging, and auditing records to determine the systems and resources affected are considered for the evaluation of estimated marginal mean along the y-axis of the graph.

Analysing organizational effectiveness in security software verification: impact of cyber-awareness training and funding allocation

Q28. What is the effectiveness of the cyber-awareness training (including practical exercises) which deal with current threat scenarios?

Q35. How effective is the verification of integrity and accuracy of security critical software? (Includes formal verification, cryptographic signatures)

Q41. To what extent does your organization ensure adequate funding for cybersecurity?

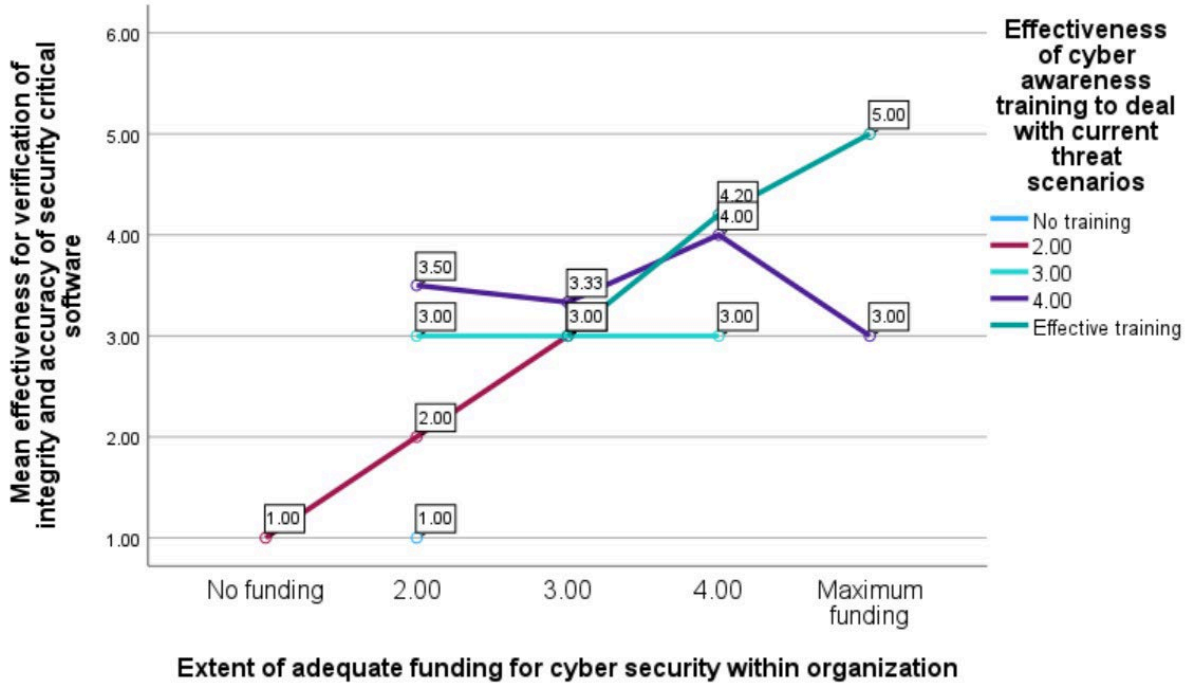


Figure 11 Mean organizational effectiveness to verify integrity of security software within the context of cybersecurity funding and cyber-awareness training

Organizations that implement effective training and provide maximum funding for cybersecurity demonstrate an estimated marginal mean of 5 for the verification of integrity and accuracy of security-critical software.

Conversely, organizations providing 'no' training and allocating less funding (2) for cybersecurity exhibit an estimated marginal mean of 1 for the verification of integrity and accuracy of security-critical software. Those with moderate training in place show no change in their effectiveness of verification, despite an increase in overall funding available for cybersecurity, with the marginal mean value remaining constant at 3.

This indicates that solely increasing funding for cybersecurity procedures will not ensure a cyberthreat-free environment. Instead, how an organization implements the training provided to their officials to utilize that training in case of a cyber threat scenario can make a difference in protecting the organization against cybercrime.

To assess organizational compliance with Incident Response, Planning, and Contingency Planning, the focus is on the implementation of practices IR7, PL4, and CP3, creating separate factors on the right side of the graph.

Furthermore, compliance with System & Communications Protection and System & Information Integrity is evaluated through the implementation of practices SC8 and SI7 respectively, contributing to the evaluation of the estimated marginal mean along the y-axis of the graph. Additionally, the implementation of Use Control, which enforces given permissions for authorized users to conduct specified actions on a system or asset and monitors their use, is considered.

Moreover, compliance with formal acknowledgment in organizational policy of the significance of cybersecurity and ensuring that operational plans and business goals adequately prioritize enhancing cybersecurity is assessed, creating factors along the x-axis of the graph.

Assessment of organizational preparedness: security operations centre in conjunction with data backups, media scanning, and boundary communication monitoring

Q32. Does your organization have a security operations centre that facilitates a 24/7 response capability that utilizes threat indicator information obtained from external organizations to review, detect and resolve threats?

Q22. Is your organization performing data backups and scanning media for malicious code before it is used in organizational systems?

Q6. How effectively are organizational communications monitored, controlled, and safeguarded at the boundaries (both external and internal) of information systems?

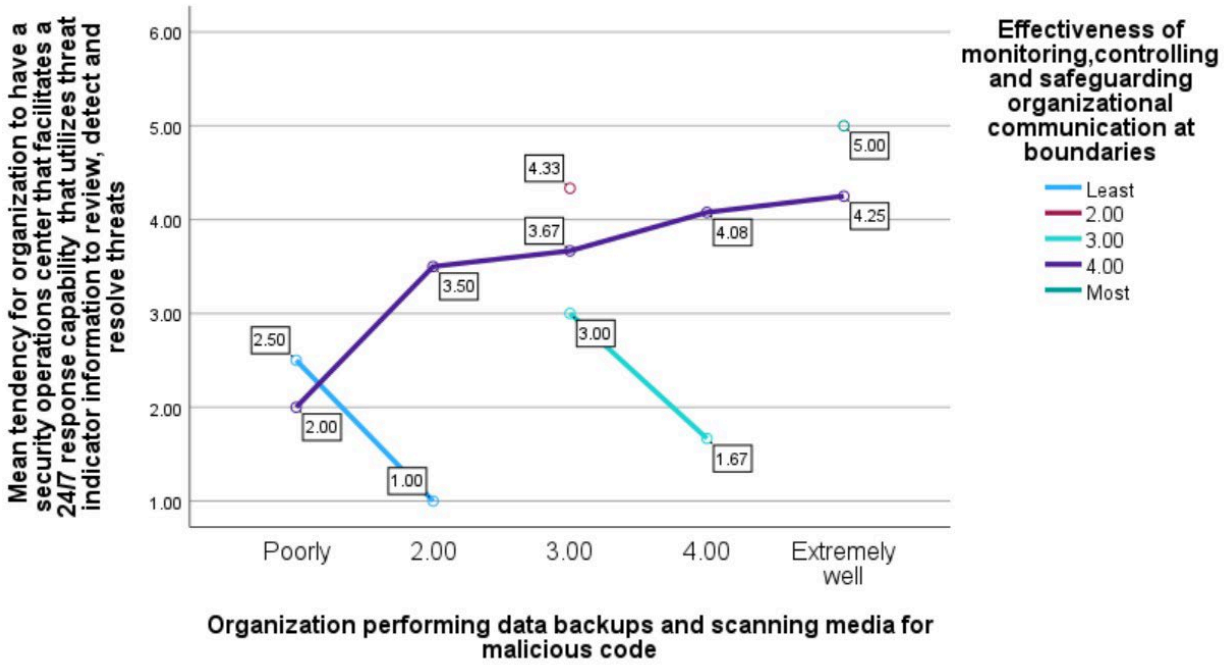


Figure 12 Mean organizational awareness to have security operations centre within the context of data backups, media scanning and organizational communication monitoring at boundaries

For organizations that excel in performing data backups and scanning media, along with effectively monitoring, controlling, and safeguarding organizational communication, the estimated marginal mean for having a security operation centre facility is 5.

Those who moderately monitor communication at boundaries exhibit an inverse relation between the implementation of level 3 practice and level 4 practice. At a moderate implementation of level 3 practice, the marginal means for performing data backups and scanning media for malicious code is 3, while at effective implementation, it is 1.67. A similar pattern is evident in the least effective monitoring of boundary communications, illustrating an inverse relationship between the implementation of level 3 and level 4, with a marginal mean of 2.5.

The minimum marginal mean value (1) is evident when there is below-average implementation of level 3 practice (performing data backups and scanning media for malicious code) and the least effective implementation of level 1 practice (organizational communications monitored, controlled, and safeguarded at the boundaries of information systems, both external and internal).

Organizations with below-average monitoring of boundary communications showcase highly effective implementation of Level 4 practice, with mean values of 4.33, even at a moderate level of data backup management and scanning.

To assess organizational compliance with System & Information Integrity, Access Control, and Incident Response, practices SI5, AC21, and IR7 respectively are evaluated, contributing to the evaluation of the estimated marginal mean along the y-axis of the graph.

Furthermore, compliance with Contingency Planning and System & Information Integrity is assessed through the implementation of practices CP9 and SI3 respectively, creating factors along the x-axis of the graph.

Moreover, compliance with Physical & Environmental Protection, Configuration Management, and System & Communications Protection is evaluated through the implementation of practices PE4, CM9, and SC7 respectively, creating separate factors on the right side of the graph.

Appendix B Analysis estimating the mean of one cybersecurity factor in relation to another cybersecurity factor

Analysis of variances (ANOVA 1) – Analysis

Q8. How often does your organization conduct periodic information system scans and real-time scans of downloaded or accessed data, or files executed from external sources?

Q34. Your organization monitors assets and determines whether logs are recorded correctly.

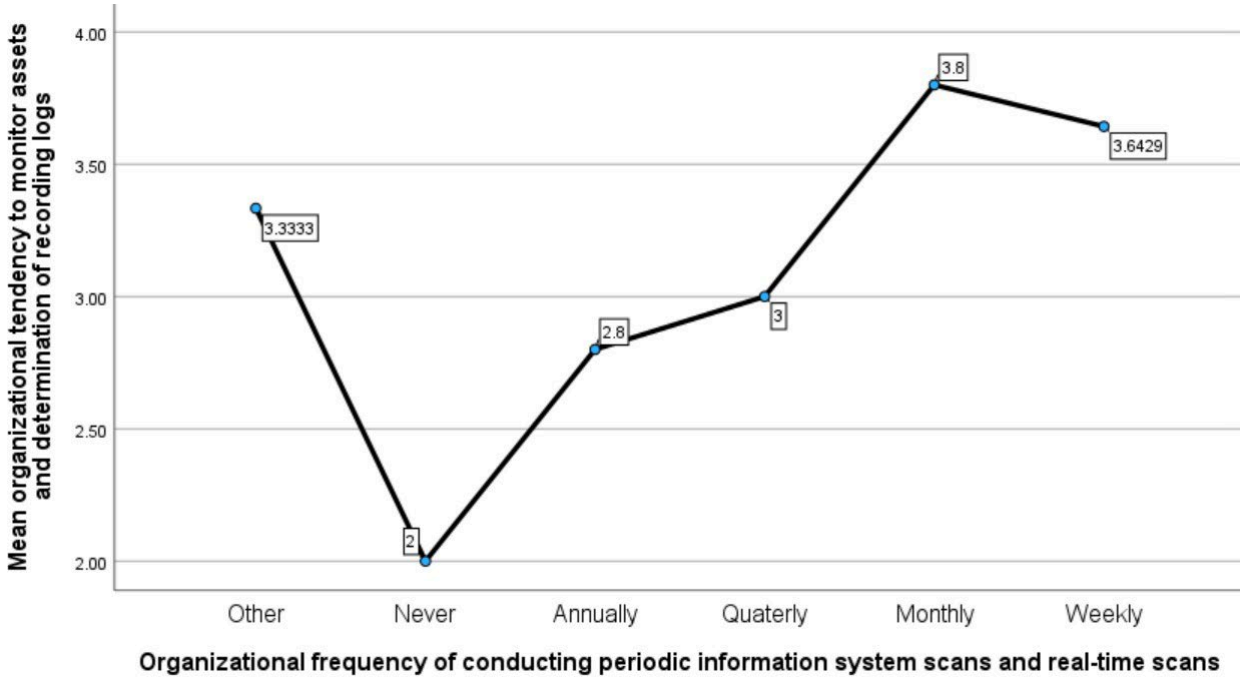


Figure 13 Mean organizational awareness of monitoring assets within the context of periodic information system scans

For organizations that never conduct periodic information system scans, the mean for monitoring assets is observed to be two (2), which is the lowest.

Conversely, organizations conducting scans weekly or monthly exhibit the highest mean for monitoring assets, with values of 3.6429 and 3.8 respectively.

The survey results indicate an increasing trend, indicating that organizations conducting system scans more frequently are more likely to monitor their assets effectively and ensure correct logging of records.

To assess organizational compliance with Risk Assessment, the focus is primarily on the implementation of practice RA5, contributing to the factor along the x-axis of the graph.

Furthermore, compliance with Contingency Planning, System & Communications Protection, and Audit & Accountability is evaluated through the implementation of practices CP6, SC28, and AU8 respectively, contributing to the evaluation of the mean along the y-axis of the graph. Additionally, emphasis is placed on aspects of automatic notifications and logging for different essential components, generated via remote level crossing status monitoring, and live reporting of failure circumstances.

Q15. How often does your organization test data backups and monitor the physical infrastructure of organizational systems?

Q22. Is your organization performing data backups and scanning media for malicious code before it is used in organizational systems?

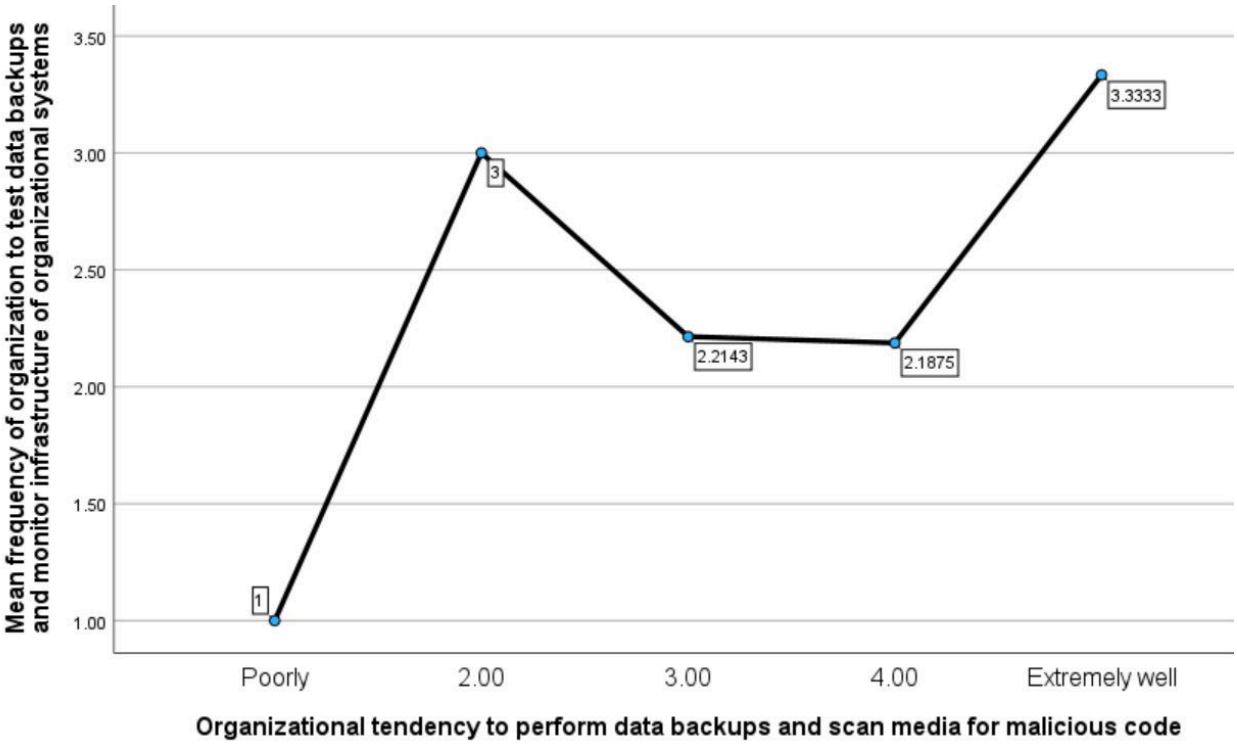


Figure 14 Mean organizational frequency to test data backups within the context of malicious code scans

Organizations that perform data backups and scanning media for malicious code extremely well exhibit the highest mean for testing those backups and monitoring physical infrastructure, with a mean value of 3.3.

Additionally, for organizations performing data backups moderately to well, poor mean values are observed for testing those backups, indicating a compromise on testing backups if backups are performed only moderately, with mean values of 2.2143 and 2.1875 respectively.

A contrast is observed for organizations choosing 2 as an option for performing data backups and scanning media for malicious codes, with their mean response to testing data backups and monitoring physical infrastructure being 3.

For organizations performing backups poorly, the tendency to test those backups is the least, with a mean value of 1.

Results indicate that for cases of poor and extremely well-performed practices, there is a direct correlation between the implementation of level 3 practices (organizations performing data backups and scanning media for malicious code before it is used in organizational systems) and level 2 practices (organizations test data backups and monitor the physical infrastructure of organizational systems). However, for low, moderate, and well-performed level 3 practices (2, 3, 4), an inverse relationship holds for performing the corresponding level 2 practice. The graph indicates that level 3 practices inversely affect level 2 practices.

To assess organizational compliance with Contingency Planning, the focus is on the implementation of practices CP6 and CP9, contributing to the evaluation of the mean along the y-axis of the graph.

Furthermore, compliance with Contingency Planning and System & Information Integrity is evaluated through the implementation of practices CP9 and SI3, contributing to the factor along the x-axis of the graph.

Q6. How effectively are organizational communications monitored, controlled, and safeguarded at the boundaries (both external and internal) of information systems?

Q39. How effective are the monitoring mechanisms used to track data-packets as they move across the organization's internet and other established boundaries?

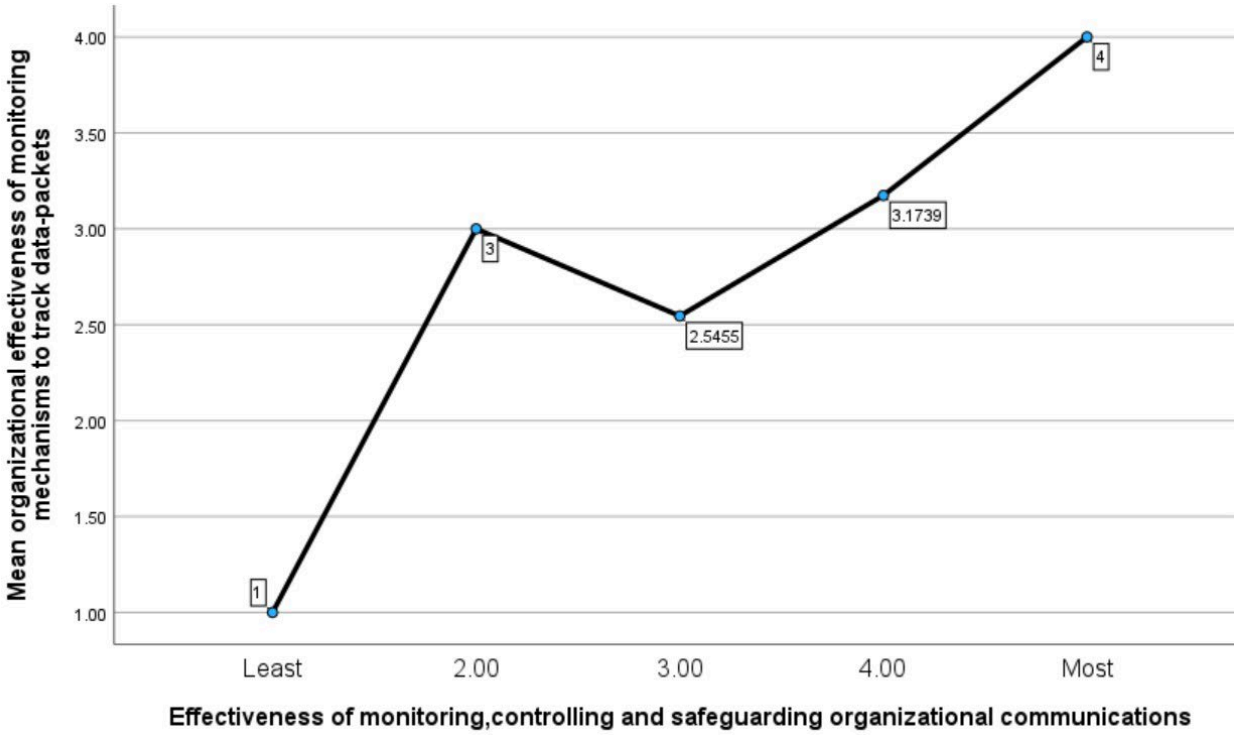


Figure 15 Mean organizational effectiveness of monitoring mechanisms to track data-packets within the context of safeguarding organizational communications

For organizations that choose 'most' to effectively control and monitor organizational communications at boundaries, the mean values for tracing data packets as they move across established boundaries are the highest, with a mean value of 4.

Conversely, organizations that choose 'least' to control and monitor organizational communications at boundaries have the lowest mean values for tracking data packets, with a mean value of 1.

Overall, survey results indicate an increasing trend, with a slight drop in mean values (2.5455) for organizations monitoring boundary communications moderately.

This indicates that overall, better implementation of level 1 practice (organizational communications monitored, controlled, and safeguarded at the boundaries of information systems) results in subsequent moderate to well implementation of level 5 practice (monitoring mechanisms for tracking data packets as they move across the organization's internet and other established boundaries).

To assess organizational compliance with Physical & Environmental Protection, Configuration Management, and System & Communications Protection, the focus is on the implementation of practices PE4, CM9, and SC7 respectively, contributing to the factor along the x-axis of the graph.

Furthermore, compliance with Audit & Accountability, Security Assessment & Authorization, Contingency Planning, and Identification & Authentication is evaluated through the implementation of practices AU6, CA2, CP8, CP9, and IA5 respectively, contributing to the evaluation of the mean along the y-axis of the graph. Additionally, emphasis is placed on practices involving planning, maintaining operations, scheduling maintenance, and enhancing computer simulation models for component and work practice design from the data obtained by Remote Condition Monitoring Systems (RCMS).

Q38. How often does your organization evaluate the efficacy of security solutions to address potential threats to the system and the organization, based on current and accumulated threat intelligence?

Q32. Does your organization have a security operations centre that facilitates a 24/7 response capability that utilizes threat indicator information obtained from external organizations to review, detect, and resolve threats?

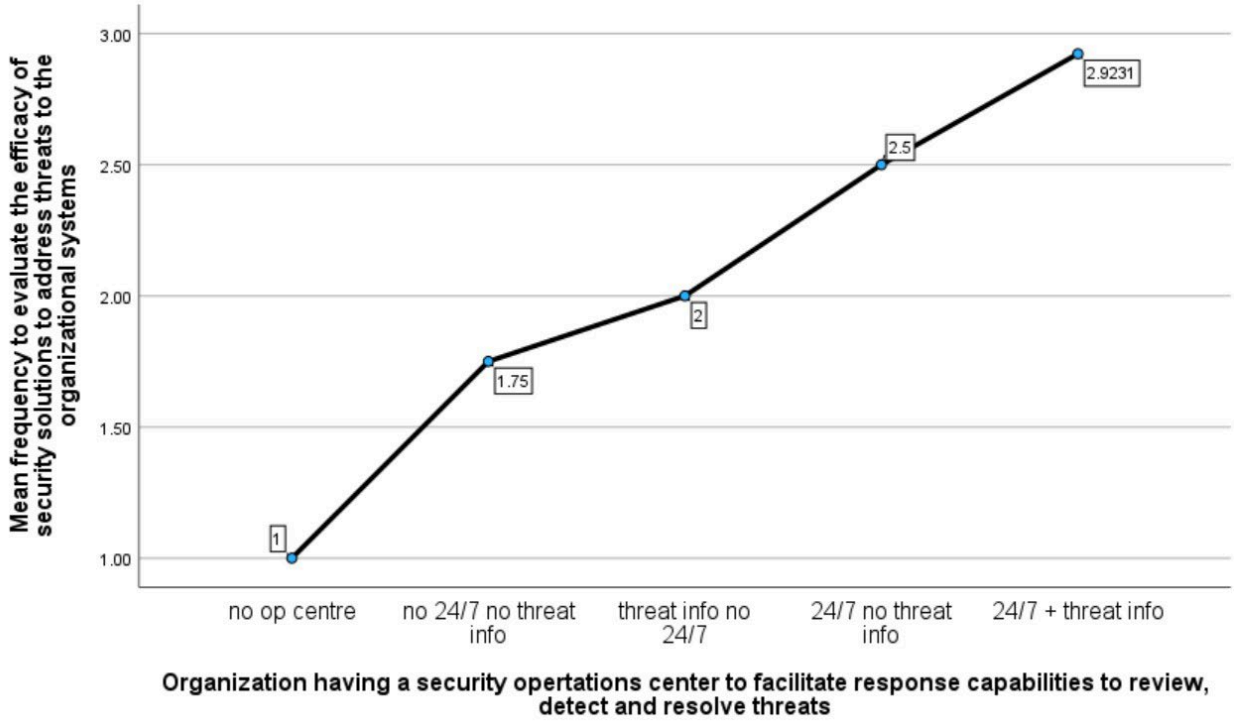


Figure 16 Mean organizational frequency to evaluate efficacy of security solutions within the context of having security operations centre

Figure 16 shows that organizations lacking a security operations centre have a mean of 1 for evaluating the efficacy of security solutions to address potential threats to the system and the organization, indicating a poor response to addressing current and accumulated threat intelligence to improve established security systems.

Conversely, organizations with a 24/7 operational security operations centre, also utilizing threat indicator information from external organizations, exhibit the highest frequency for evaluating the efficacy of security solutions, with means being 2.9231.

Survey results reveal a direct linear relationship between having an operations centre and the frequency of evaluating and improving security solutions, indicating a direct correlation between the implementation of practices from level 4 and level 5. However, in this case, an efficient implementation of level 4 practice (organization having a security operations centre that facilitates a 24/7 response capability that utilizes threat indicators to review, detect, and resolve threats) only leads to a moderate implementation of level 5 practice (organization evaluating the efficacy of security solutions to address potential threats to the system and the organization, based on current and accumulated threat intelligence) at most.

To assess organizational compliance with System & Information Integrity, Access Control, and Security Assessment & Authorization, the focus is on the implementation of practices SI5, SI2, AC17, AC21, and CA1 respectively, contributing to the evaluation of the mean along the y-axis of the graph.

Furthermore, compliance with System & Information Integrity, Access Control, and Incident Response is evaluated through the implementation of practices SI5, AC21, and IR7 respectively, contributing to the factor along the x-axis of the graph.

Q4 Only authorized personnel are provided physical access to the organization's information systems, equipment, and working environments?

Q5. How often are audit logs of physical access examined?

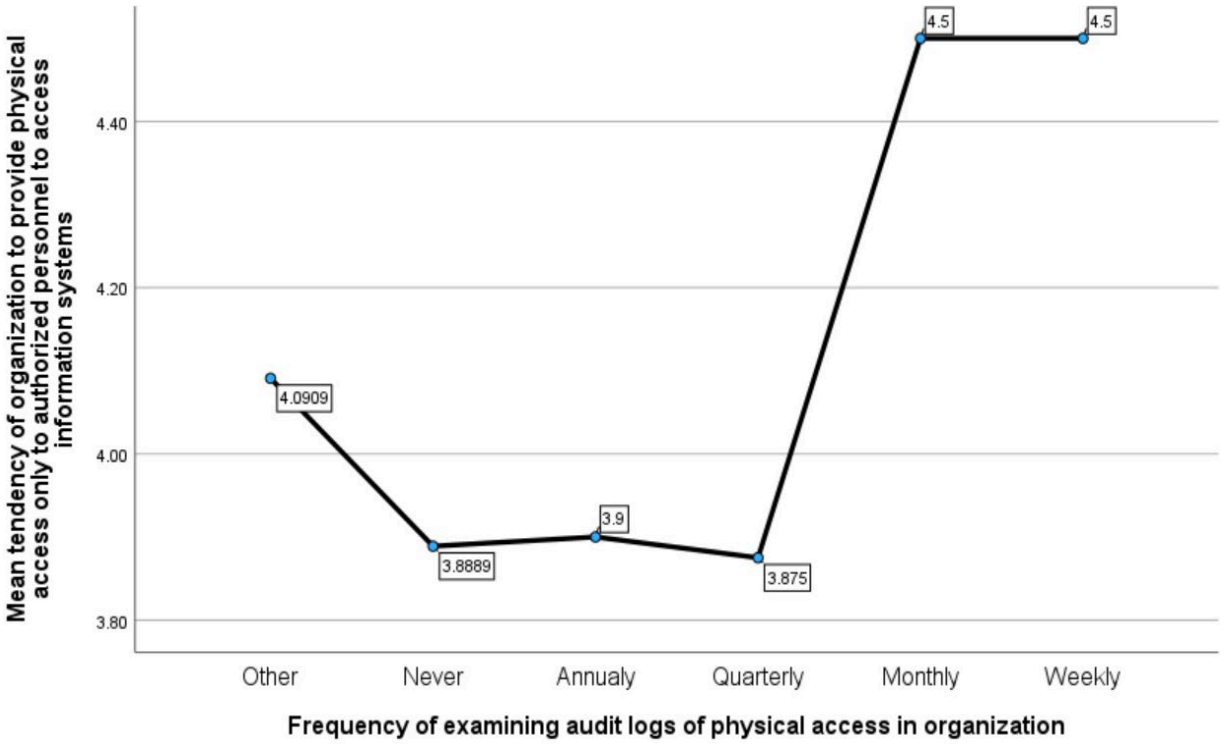


Figure 17 Mean organizational awareness to provide physical access within the context of examining physical access audit logs

Figure 17 shows that the overall mean of only authorized personnel being provided physical access to the organization's information systems, equipment, and working environments is high.

Organizations considering auditing logs never, annually, and quarterly exhibit a consistent mean of 3.8889, 3.9, and 3.875 respectively. However, organizations auditing logs monthly and weekly have a higher mean value of 4.5.

There is not a significant change in means of authorized personnel being provided access to information systems when the organization audits physical access poorly to a moderate level. However, as the audit logs for physical access are examined effectively, the means increase substantially, indicating stricter restrictions on physical access.

To assess organizational compliance with Personnel Security, the focus is on the implementation of practices PS1-8, contributing to the evaluation of the mean along the y-axis of the graph. Additionally, security perimeters are established and enforced to safeguard rail systems as well as any related auxiliary systems, software, or hardware. Rail systems can require the same degree of physical protection as critical operating areas.

Furthermore, compliance with Audit and Accountability is evaluated through the implementation of practice AU4, contributing to the factor along the x-axis of the graph.

Q6. How effectively are organizational communications monitored, controlled, and safeguarded at the boundaries (both external and internal) of information systems?

Q23. How often does your organization monitor security controls, develop, and implement risk assessment/ mitigation plans?

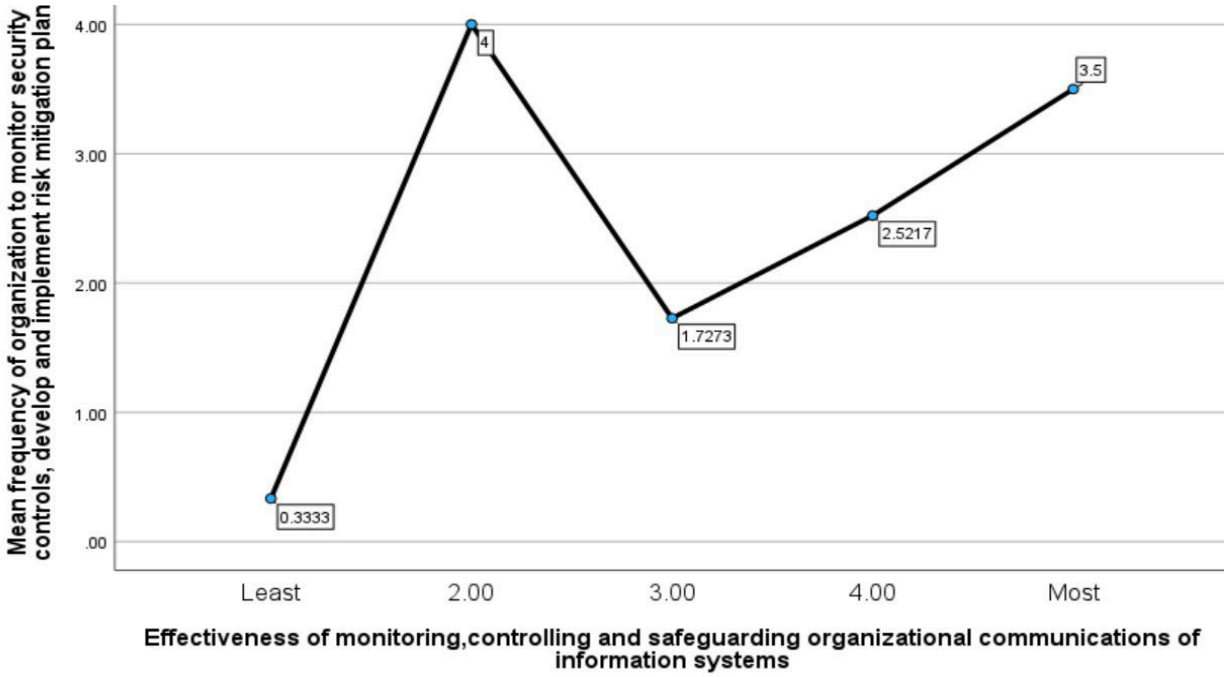


Figure 18 Mean organizational frequency to monitor security controls within the context of organizational communications of information systems

Figure 18 shows an increasing trend and a direct correlation between monitoring, controlling boundary communications, and developing risk assessment plans.

However, it is noted that officials from some organizations have identified that even if their organization might not necessarily be controlling and safeguarding boundary communications, they rigorously monitor security controls and develop risk and mitigation plans, with the highest mean value of four (4).

Conversely, for other organizations, the survey results show that the implementation of organizational communications monitored, controlled, and safeguarded at the boundaries influences the organization's ability to monitor security controls and develop and implement risk assessment/mitigation plans.

In cases of moderate effectiveness of monitoring, control, and safeguarding at the boundaries, the mean value of monitoring security controls is lower, at 1.7273.

However, for organizations with the most effective monitoring, control, and safeguarding at the boundaries, the mean value increases to 3.5.

To assess organizational compliance with Physical & Environmental Protection, Configuration Management, and System & Communications Protection, the focus is on the implementation of practices PE4, CM9, and SC7, contributing to the factor along the x-axis of the graph.

Furthermore, compliance with Physical & Environmental Protection and Risk Assessment is evaluated through the implementation of practices PE9-16 and RA1 respectively, contributing to the evaluation of the mean along the y-axis of the graph. Additionally, threats that potentially affect rail systems must be addressed using good practices and mitigation techniques to avoid or lessen their effects on vital assets and train operations.

Appendix C Survey information

Griffith UNIVERSITY
Queensland, Australia

Cyber Security for Railway Industries
INFORMATION SHEET
GU Ref No: 2022/293

Senior Investigator: Professor Ernest Foo, Dr Sharmistha Dey, Dr Mardé Helbig
Student Researcher: Ojaswini Malhotra
Department: School of Information and Communication Technology, Griffith University
Phone: 0451 840 671
Contact email:

e.foo@griffith.edu.au s.dey@griffith.edu.au m.helbig@griffith.edu.au
ojaswini.malhotra@griffithuni.edu.au

Why is the research being conducted?

This is a survey-based student research project in the field of cyber-security aimed at railway industries and their provisions to set up cybersecurity controls. This survey has been developed under the guidance of the research supervisor, Professor Ernest Foo, who has experience in the field of cybersecurity and computer networking, Dr Sharmistha Dey who has extensive experience with Enterprise Systems and implementation of large business software and Dr Mardé Helbig who has experience in solving dynamic multi-objective optimization problems using computational intelligence algorithms, decision making and visualization. The purpose of this survey is to learn the applications of cybersecurity standards in real time scenarios within the railway industry.

What you will be asked to do

Participants will be asked to complete an online survey, making sure that any confidential information regarding them and their organization is not disclosed. This research project will focus on 5 Cybersecurity Maturity Model Certifications (CMMC) Levels and how different aspects of each level are being implemented within the railway industry. The questions in the survey will be segregated according to the 5 CMMC levels:
Level 1 – Basic Cyber Hygiene
Level 2 – Intermediate Cyber Hygiene
Level 3 – Good Cyber Hygiene
Level 4 – Proactive
Level 5 – Advanced/Progressive

The basis by which participants will be selected or screened

Potential participants of this survey are railway authority officials. All types of railway sectors will be taken into consideration for this survey whether large scale or small scale.

Risks to you

There is no compensation for responding to this survey nor is there any known risk.

The expected benefits of the research

The data collected will provide useful information regarding cybersecurity measures within railway sectors. The response received from multiple railway sectors will help in coming up with a conclusion regarding the extent to which railway facilities are compliant with cybersecurity protocols and with different levels of the CMMC model.

Your confidentiality

In order to ensure that all information remains confidential, the survey will not collect any personal details. Research data (survey responses and analysis) will be retained in a password protected electronic file at Griffith University for a period of five years from the date of the final publication before being destroyed.

Your participation is voluntary

Participation in the survey is strictly voluntary, and you may refuse to participate at any time. Completion and return of the survey will indicate your willingness to participate in this study.

Questions / further information

If you require additional information or have questions, please contact the research team via email:

Professor Ernest Foo: e.foo@griffith.edu.au

Dr Sharmistha Dey: s.dey@griffith.edu.au

Dr Mardé Helbig: m.helbig@griffith.edu.au

Ojaswini Malhotra: ojaswini.malhotra@griffithuni.edu.au

The ethical conduct of this research

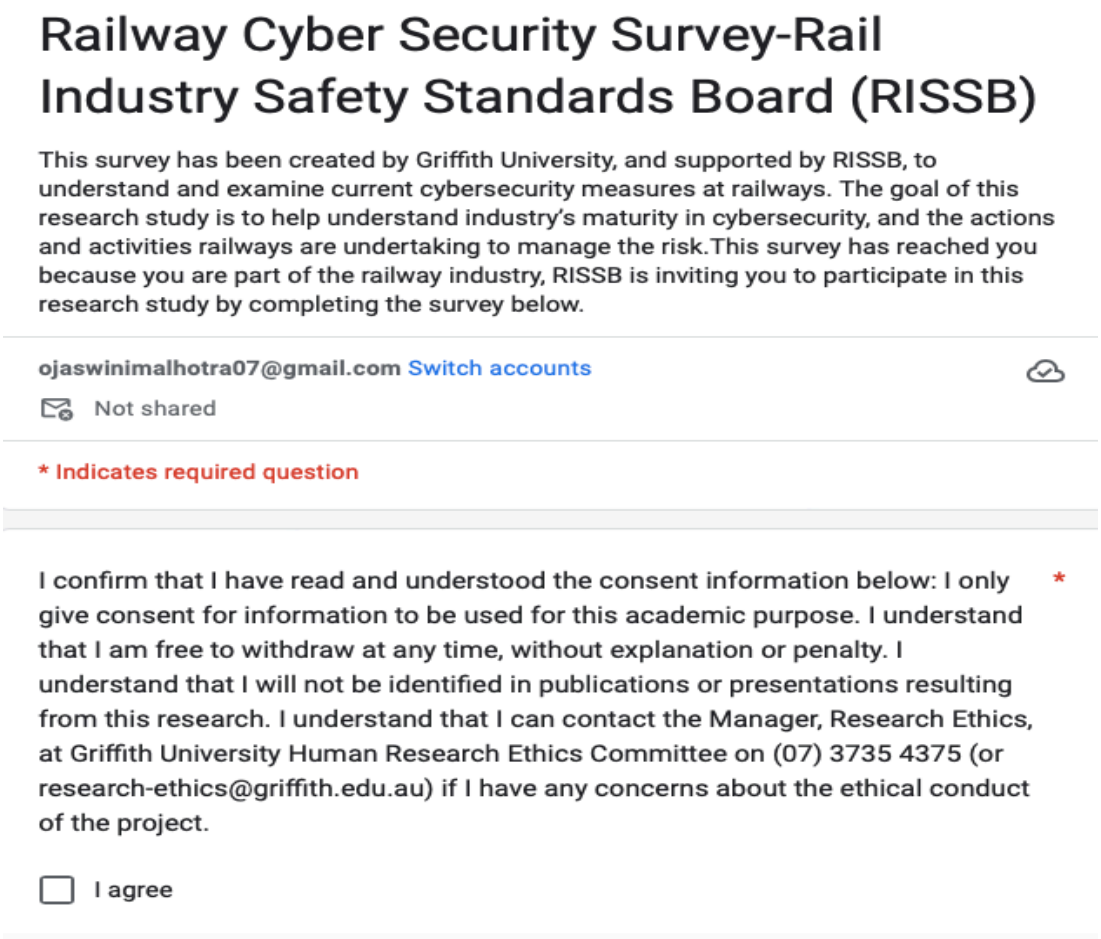
Griffith University conducts research in accordance with the National Statement on Ethical Conduct in Human Research. If you have any concerns or complaints about the ethical conduct of this research project, you are encouraged to contact the Manager, Research Ethics on 07 3735 4375 or research-ethics@griffith.edu.au.

Feedback to you

Research results will be reported in an academic thesis and may also be disseminated via journal articles and/or conference presentations. Please email the research team if you would like a summary of the research findings.

Completion of this survey will be taken as your consent to participate in the research.

Survey consent questions



Railway Cyber Security Survey-Rail Industry Safety Standards Board (RISSB)

This survey has been created by Griffith University, and supported by RISSB, to understand and examine current cybersecurity measures at railways. The goal of this research study is to help understand industry's maturity in cybersecurity, and the actions and activities railways are undertaking to manage the risk.This survey has reached you because you are part of the railway industry, RISSB is inviting you to participate in this research study by completing the survey below.

ojaswinimalhotra07@gmail.com Switch accounts

Not shared

* Indicates required question

I confirm that I have read and understood the consent information below: I only give consent for information to be used for this academic purpose. I understand that I am free to withdraw at any time, without explanation or penalty. I understand that I will not be identified in publications or presentations resulting from this research. I understand that I can contact the Manager, Research Ethics, at Griffith University Human Research Ethics Committee on (07) 3735 4375 (or research-ethics@griffith.edu.au) if I have any concerns about the ethical conduct of the project. *

☐ I agree

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

For information regarding products developed by RISSB contact:
Rail Industry Safety and Standards Board

Brisbane Office
Level 6, 200 Creek Street
Brisbane, QLD, 4000

PO Box 518
Spring Hill, QLD, 4004

T +61 7 3724 0000
E Info@rissb.com.au