Railway Cybersecurity: Capabilities, Challenges, and Prospects

Arash Aziminejad, Chief Engineer-Data Communications
WSP

Yayati Kaushik, Senior Systems Engineer
WSP

Paper prepared for presentation at the
CAV READINESS (PART 2): DIGITAL INFRASTRUCTURE Session
at the 2020 TAC Conference & Exhibition

Abstract

The rail transport networks have become overwhelmingly digital, with a diverse range of data traffic flowing across systems to track, monitor, and control both electronic/electrical and mechanical subsystems. Introduction of advanced electronic platforms and communications across networks supporting mission-critical public services have significantly emphasized the challenge for detection, containment, and remediation of possible disruptions. Furthermore, as the tendency for Internet-of-Things grows among field hardware and control systems, the added vulnerabilities further augment the potential for availability outages and hostile or non-premeditated disruptions to physical assets. This presentation aims to establish characteristics of a comprehensive, holistic, and integrated cybersecurity framework in the context of rail transportation, where instead of the traditional data protection and privacy concerns, the focus revolves around safety, integrity, and operational resilience. As a main contribution of the presented research, the planning challenges involved with implementation of an enterprise-wide cybersecurity risk mitigation methodology are investigated at both strategic and tactical levels, and based on lessons learned from practical real-life project scenarios, best practices recommendations are proposed to more efficiently mitigate the cyber risk and enhance safety, availability, and integrity of the protected networks and physical assets.

Introduction

Digital integration, Internet-of-Things (IoT), and Big Data concepts are pushing public mission-critical data networks (i.e., data networks whose failure result in the failure of business operations which make them critical to the organization's mission such as the train control system) toward further openness, interconnectivity, and interoperability. This means the traditional "stick to a closed network architecture to keep it secure" approach risks forfeiting many of the benefits of a modern communication IP network [1]. In a safety-driven mission-critical environment like railways, there is a de facto motivation and excuse for sustaining outdated technology. Furthermore, there are inherent security vulnerabilities that can compromise integrity and performance of "secure closed-architecture" data networks, including removable media, "man-in-middle"-type attacks, and infected replacement servers/components [2].

The current sensitivity about the global state of network security in general can be inferred from the following set of statistics:

1. In 2018, the Identity Theft Resource Center counted a 24% decrease in the number of breaches but a 226% increase in the number of records exposed. The total number of records exposed was more than 446 million [3].
2. 80% of cybersecurity and IT experts anticipate a "catastrophic" data breach at their companies by 2021 [4].
3. Only 19% of businesses are highly confident in their organization's ability to mitigate and respond to a cyber event [5].
4. 57% of breached companies have to be informed of the breach by someone else, such as law enforcement, partners, customers [6].
5. 2017's cyber breach costs increased by 22.7% over 2016 [7].

In the context of providing a realistic and reliable basis of comparison for the specific case of cybersecurity threat vectors for rail transportation applications, project Honeytrain was created [8]. The objective was to set up a virtual train control and rail operation system as a honeypot for hackers to evaluate tangibility of cyber risk to the rail industry. The virtual rail infrastructure was reproduced using real hardware, communication protocols, operator workstations, and a customized website with general information. All the operational activities including CCTV video feeds of real stations, train schedules, timetables, ticketing, and information about train disruptions were simulated for six weeks. Logins and passwords were left at their defaults and no security measures were enabled. The following results and deductions were obtained from the project:

1. There was an alarming total of 2.7 million attacks on the system.
2. Approximately 61% of attempted attacks occurred on the media server and firewall components.
3. The majority of attacks were carried out against login/passwords as automated dictionary attacks.
4. Some attackers were proven to possess deep knowledge of the industrial control systems involved and there were a few cases of total system compromise by such attackers (i.e., attackers managed to reach the configuration of industrial or safety-critical components).

The analysis of results indicated that through relatively light security measures (e.g., robust passwords, firewalls, security awareness) a significant portion of attempted attacks can be prevented. Rail systems are a prime target for terrorists, such as those who conducted the 2004 Madrid railway bombing. Further, extortion attempts on San Francisco Muni system in 2016 and Germany's Deutsche Bahn railway system in 2017 are examples of ransomware attacks. Other examples of known and successful cases of railway system cyberattacks include the 2003 CSX US railway system worm attack which caused nearly a day's worth of delays along the CSX's entire East Coast rail operations, the 2008 Lozd (Poland) tram system hacking where a 14-year old controlled key points of the tram's track through a modified TV remote control (4 trains were derailed injuring 12 people), and the 2015-2016 UK rail system cyberattacks (at least 4 cyberattacks on rail systems were identified as preparations for attackers to establish a presence for future exploitations).

This research intends to investigate the increased level of cyber risk to critical rail infrastructure assets and establish an industry-oriented framework to manage the growing cyber threat. Since cybersecurity is an evolving discipline driving not just the need to identify the risks but also to understand the threats and opportunities these risks present, systems should be assessed for vulnerabilities to identify the most appropriate ways to introduce security measures to protect the environment through a set of technical, procedural and managerial safeguards and countermeasures. Considering the ever-evolving nature of cyber threats, cybersecurity capabilities must be continuously developed and assessed to keep abreast of the hostile environment. Finally, an effective, reliable and resilient security program needs to be planned and launched to limit damages from security incidents, i.e., efficiently respond to and recover from successful cyber-attacks.

Railway Cybersecurity Challenges and Threat Vectors

A cybersecurity attack vector is a path or means by which an attacker can exploit system vulnerabilities, i.e., gain unauthorized access to a computer or network to deliver a payload or malicious outcome. The total number of attack vectors an attacker can use to manipulate a network or computer system or extract data is termed as the attack surface. In the general IT domain, cybersecurity attacks can be classified based on the interaction approach with the target, their goals and the methodology used during the attack. General categories include passive (does not require any interactions with the target or the network under attack) and active attacks (interacts directly with the target or with the network to cause intentional malfunctioning). Most attacks exploit an inherent vulnerability within one or more components or interface of the System. A typical modern-day railway system has numerous subsystems and myriad interfaces between those subsystems, providing a large attack surface to the would-be attackers.

System vulnerabilities are weaknesses in control systems, information systems, system procedures, controls, or implementations that can be exploited by a threat source. Such vulnerabilities can result from many sources, including policy/procedure, architecture/design, configuration/maintenance, physical intrusion, software development, communication/network, and lack of training/awareness. Some vulnerabilities are general to IT systems and products such as wireless/cellular communication, integration of physical and virtual layers, and increasing levels of automation. In contrast to general vulnerabilities, some vulnerabilities are specific to rail transportation systems and applications including strict mission-critical and safety requirements, mapping of networked technology across large-scale rail transportation systems, interdependencies among different subsystems, and access to huge amounts of real-time data. Some of the vulnerable points within railway systems include:

1. Industrial control hardware, firmware, software and protocols
2. RFID, Wi-Fi, TETRA and LTE based radio systems, used for transmitting operational data
3. Remote installations of communications and control infrastructure
4. Fare payment and validation systems, which are interfaced to the banking infrastructure
5. Interfaces with external agencies or entities for exchange of real-time operational data.

Cybersecurity threats can be politically (e.g., nation states cyber warfare, cyberterrorism, and hacktivists) or commercially (e.g., an individual wants to obtain financial/business-related information) motivated, insider threat agents stemming from employees and 3rd party service/product providers (e.g., data subcontracting compromise resulting in the loss of data control), and/or due to human factors (e.g., improper training, negligence, and/or lack of awareness). Types of threats include data theft (stealing valuable information or data residing at transit site locations or secondary storage locations), data integrity breaches (possibility of critical data to be compromised or tampered with), and availability-rejection of access (due to attacks that trigger denial of service). Table I presents a more detailed description of possibility of different cyber-attacks linked to source of attacker, his intention and the compromised security element [9]. The high-level list of hazards pertaining to cybersecurity vulnerabilities and the accompanying cyber-attacks include:

1. train collision
2. derailment
3. service disruption/performance degradation
4. threat to the safety of workforce, passengers, and public resulting in harm
5. financial loss
6. failure to comply with law
7. criminal damage
8. reputational damage to railway systems due to leakage of sensitive information and/or any of the examples above.

Cyber-attack	Source	Actor	Action	Security element
Tapping, snooping, scavenging, shoulder surfing and traffic analysis and traffic operational data.	Internal or External	Human	Malicious	Confidentiality
Modification, Masquerading, Replay and Repudiation of acquired data	Internal or External	Human	Malicious	Integrity
Denial of service attacks, Riot/Civil Disorder, arson, Labor Unrest, Procedural Violation	Internal or External	Human	Malicious	Availability
Careless use of wireless networks, posting information to discussion boards and blogs, sending sensitive information via e-mail and instant messaging, Improper disposal of sensitive media and failing to log off before leaving workstation	Internal	Human	Non-malicious	Confidentiality
Failure and maintenance data entry errors and omissions	Internal	Human	Non-malicious	Integrity
Programming errors, including syntax and logic problems	Internal	Human	Non-malicious	Availability
Compromising emanations, eavesdropping, takeover of authorized session	Internal or External	Technological	Non-malicious	Confidentiality
Jamming (telecommunications)	Internal or External	Technological	Non-malicious	Availability
Faults in power supply and data networks	Internal	Technological	Non-malicious	Availability
Earthquakes, hurricanes, wind, flood, Tsunami, fire, lightning, animals and wildlife	External	Natural disaster	Non-malicious	Availability

Table I: Cyber-attacks linked to the source of attacker, his intention and the compromised security element

A main source of rail systems cybersecurity challenges, which in turn can become the root cause for vulnerabilities and risks, is the ever-growing tendency toward full convergence of the information and operations technologies. A significant portion of the cited challenges can be traced back to the gigantic amounts of data generated from various network-monitoring devices and the necessity for new processing techniques to manage detected vulnerabilities and cyber alerts that help improve general computer security and wellbeing [9, 10, 11]. Some key cybersecurity-related challenges within an intelligent public rail system in reducing and containing the attack surface can be summarized as:

1. Difficulties to absorb and incorporate security into safety due to insufficient understanding of modern cybersecurity concepts and acquiring the required skills to implement security.

2. Inadequate emphasis and investment assigned to security, cybersecurity is often an after-thought in public rail transportation startup/expansion projects.

3. Insufficient investigation, planning, and analysis for realizing optimal countermeasures.

4. Slow phasing out of vulnerable safety-oriented legacy systems makes proper maintenance and updates an important security consideration, especially when phasing out these systems becomes difficult or unfeasible.

5. Inefficient exchange of information between the public rail system and Smart Cities' operators.

6. Inadequate situational awareness (i.e., being aware of what is physically happening around you, where you are supposed to be, and whether anyone/anything around you is a threat to your health and safety).

7. Resistance to adoption of modern security principles and techniques (added security is equal to added network complexity).

8. Staff with only domain-specific expertise favored in rail transportation agencies' recruiting patterns.

Requirements for Achieving Rail Transportation Cybersecurity Vision and Goals

Requirement Category	IT	ICS
Performance	• Non-real-time • Response must be consistent • High throughput is demanded	• Real-time • Response is time-critical • Moderate throughput is acceptable
Availability/ Reliability	• Responses such as rebooting acceptable • Availability deficiencies can be tolerated	• Responses such as rebooting not acceptable • Availability deficiencies cannot be tolerated, outage must be planned
System Security	• The priority sequence of security concept values is Confidentiality, Integrity and Availability	• The priority sequence of security concept values is Availability, Integrity and Confidentiality
Risk Management	• Manage data • Data confidentiality/integrity are paramount • Major risk impact: delay of business operations and financial loss	• Control physical world • Human safety is paramount • Major risk impact: non-compliance, environmental impacts, loss of life, equipment, or production
System Operation	• Designed to be used with typical Operating Systems • Upgrades are straightforward and usually automated	• Proprietary Operating Systems with limited built-in security capabilities • System upgrades are cumbersome to test and deploy, requiring scheduled downtimes and maintenance windows, interrupting normal operation
Communications	• Standard communications protocols • Primarily wired network with localized wireless	• Many proprietary and standard communications protocols • Diverse communication media including dedicated wired/wireless
Change Management	• S/W changes are applied in a timely fashion in the presence of good security policies/procedures	• S/W changes must be thoroughly tested and incrementally deployed to ensure that integrity of control system is maintained
Managed Support	• Allows for diversified support styles	• Service support is usually via a single vendor
Component Lifetime	• Lifetime on the order of 3 to 5 years	• Lifetime on the order of 10 to 15 years, or more
Component Location	• Components are usually local and easy to access	• Components can be isolated, remote, and require extensive physical effort to gain access to them

Table II: Summary of design, operation and maintenance requirements differences between the ICS and IT systems

In today's technological nomenclature, the term IT indicates the use of hardware/software computational platforms to create, store, transmit and retrieve data, created through enabling business processes. On the other hand, Operational Technology (OT), or equivalently, the Industrial Control Systems (ICS) is the use of hardware/software computational platforms to detect, monitor or control the physical devices, processes, and events in an industrial enterprise. The difference between the OT and ICS is subtle; the ICS is a major segment within the OT sector, which comprises systems that are used to monitor and control industrial processes. An ICS is often managed via a Supervisory Control and Data Acquisition (SCADA) systems that provides a graphical user interface for operators to easily and swiftly observe the status of a system, receive any alarms indicating out-of-band operation, or enter system adjustments to manage the process under control. An ICS system will typically consist of SCADA, Programmable Logic Controllers (PLCs), and distributed installations of sensors and relays in the field.

During the past two decades the rail transportation industry has experienced explosive growth in automation of services and operations across the IT, OT and Industrial Internet-of-Things (IIoT) subdomains, as well as in the SCADA systems and the ICS. In rail transit systems, IT and OT are set up, used, and controlled based on different requirement sets but often converge. Consequently, security measures are different for them as well. Understanding the cited differences is key to keeping both systems secure and avoiding potential conflicts. Table II provides a summary of differences between design, operation and maintenance requirements between the ICS and IT systems.

Developing a successful comprehensive organizational security plan needs a break-down of efforts into strategic and tactical levels. In a nutshell, tactical planning is designed to be near-term and relatively low-cost improvements providing organizations a significant return of investment whereas strategic planning often requires more time, effort, resources and sometimes cost, but often helps complete the long-term vision for an organization's security goals. The remaining of the section is devoted to further elaborate these two concepts in the context of rail transit systems.

A. Strategic Level

In the general sense, cybersecurity is no longer considered to be a purely IT/technological issue. Effective cybersecurity is an enterprise-wide topic that requires addressing through an interdisciplinary approach, and needs a comprehensive top-to-bottom governance commitment for planning, implementation, enforcement and maintenance to ensure all business aspects are aligned to fully support the end business strategy and objective [12, 13]. A reliable, thorough, and end-to-end organizational security framework needs to comprehensively cover the following areas:

1. *Policy/Governance*: Business requirements define and control specific cybersecurity components. Standards, procedures and guidelines which complement the organizations cybersecurity policy must be developed.

2. *Compliance*: The cybersecurity territory is bound by both government regulations (e.g., Homeland Security Act/FISMA, and the CSA Staff Notice 11-332 titled "Cyber Security" in Canada) that shape and quantify cyber-defense techniques and industry standards that set requirements for conduct (e.g., NIST SP800-12/14/37/53 CENELEC EN50159, and NERC-CIP Standards).

3. *Threat Intelligence*: Establishes potential present and future hazard scenarios for which security countermeasures/safeguards must be prepared. The required information is extracted from

media, governments, industry/business partners, security suppliers, internal efforts, or a combination thereof.

4. *Holistic Approach*: Integrated corporate security activities related to cybersecurity/logical security, physical security, and administrative/personnel security collectively provide the aggregated elements of an effective and end-to-end protective solution. In other words, logical/technology-based cybersecurity is considered an integral part of the general security package. Cybersecurity technology underpins but does not control an effective security policy. In practice, however, technology is frequently viewed as the solution rather than a mere component of a broader strategy. Areas of special interest in planning a holistic cybersecurity program include:

    a. *Third-party systems*: Functional systems may include transfer of data to and from, or through third party systems/interfaces, which makes data security requirements essential during the process.
    b. *Interfaces:* Security measures and constraints must be set between organization's (i) internal systems and external interfaces and (ii) internal sub-systems, which also helps in creating a network/system segmentation for improved security.

5. *Integrated Framework*: Acts as the overarching security governance and management framework integrator which amalgamates other latest relevant standards, frameworks, and practices used through providing a technology-agnostic common language.

The process of cybersecurity strategic planning for a rail transportation system starts from responding to the key questions which help define the cybersecurity program objectives' broad picture including the threat landscape and all the components of the risk and proportional mitigation and recovery processes which need to be developed, commissioned, and maintained. Table III lists some of the cited critical key questions.

An effective cybersecurity program commences through articulating a strategy in response to the key planning questions, supported by an assessment of the organization's current preparedness in facing cyber threats, margin for risk, and quantification of financial exposure. In response to the highly volatile nature of threat vectors, all organizations managing security risks on behalf of rail industry staff and passengers should have formal, dynamic, recurring, and comprehensive risk management systems in place [10, 14]. The risk assessment methodology must allow the understanding of different physical and cyber systems, technologies, and their developments in the rail mode. Specific areas to consider for planning a risk management platform include:

1. *Triangle association with Governance/Compliance*: Based on the strategic responsibilities of support, define and direct, the Governance provides the risk control mechanism input to a risk management platform. Furthermore, the compliance requirements inputs (legal, industry standards and license agreements) are equivalently essential for a reliable risk control management platform.

2. *Adaptation to rail transportation systems:* Application-based cybersecurity protection design (scoping and tailoring) aims for rail transportation safety and safety management. An efficient risk control management platform needs to follow the same principles.

Asset Criticality	• Which assets are most important to a rail transportation system? o From the service continuity/safety point of view o From the supply chain point of view • What are the principal assets to be protected/preserved? o Infrastructure/communications o Instrumentation and control (hardware and software) o Critical data (e.g., sensor information, logs, asset information and databases, personal, etc.)
Threats	• Which assets are attractive to different threat actors? What loss scenarios can be enacted? What attack approaches/methods can be utilized? • What are the components of the threat vector/landscape for a specific rail transportation system?
Preparedness	• What policies and control frameworks need to be in place to counter/mitigate cyber risks? • What governance arrangements are needed? • Organizational roles and responsibilities – Who is responsible for what? • What cyber-attack detection and protection mechanisms need to be utilized? • What cybersecurity awareness and training programs are to be implemented? (Who gets what training and how often? How often is the training evolved or revamped?)
Response	• What response procedures/documentations are needed for business continuity? How do the procedures need to be tailored based on the nature of the attack and attacked asset? • How will the communication and coordination be managed? o Across different sectors of a specific rail transportation system o With 3rd parties, customers, and the media o With law enforcement/government authorities
Recovery	• What are the procedures/controls required for disaster recovery? What are the arrangements/task force formations for clean-up and recovery operations? • Under what conditions can a "full recovery" state be declared?
Evolve	• What, how and how often are adjustments to be made to the organization's cybersecurity program in response to the changes in assets, risks and threats?

Table III: key questions to define the threat landscape and all components of the risk, mitigation, and recovery processes

3. *Legacy, current, and whole life–cycle systems*: Risk assessment processes for new systems need to encompass all stages of corresponding life cycles from design to decommissioning and disposal. Legacy systems need to be assessed for vulnerabilities from their current state through to decommissioning and disposal.

4. *Review/future-proofing*: Risks are not stationary and must be periodically reassessed. Risk assessment should be an integral part of future-proofing work, seeking effective responses to future needs, requirements, and challenges.

The traditional approach of the "blind" hardening of inherently vulnerable systems against known and identified cybersecurity threats has proven to be only partially effective. This is particularly true for large, complex, and geographically dispersed systems deployed for rail transportation applications. Identification of all critical assets and components to be protected for a rail transportation application is a cumbersome process, and it becomes increasingly complex and expensive to harden every aspect of a system against all types of cyber threats. Therefore, a smart and adaptive approach to cybersecurity protection for rail transportation systems needs to include a multi-faceted multi-objective strategy of prevention and mitigation through improved system resilience, which is a system's ability to recover or regenerate its performance after a degradation caused by a successful cybersecurity attack. The key words in this challenge are, "detect, respond, and recover". From a strategic prospective, system security planning needs to provide adequate and comprehensive responses to business continuity/disaster recovery requirements.

B. Tactical Level

The nature of the cyber adversary against public infrastructure has changed in recent years. The evolution is projected in introduction of new terminology including "advanced persistent threat", which refers to an adversary that possesses sophisticated levels of expertise and significant resources, allowing it to create opportunities to achieve its objectives by using combined attack vectors (e.g., cyber, physical, and deception) [15]. The advanced persistent threat pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives. From a tactical point of view, design of security controls for rail transportation systems aims to counter and nullify such a level of adversary.

Any cyber ecosystem is only as secure as its weakest link, so when the IT and OT including all relevant subdomains converge, a vulnerability in one or at the point of intersection can impact the security posture of the entire fusion. Due to specific and stringent safety-critical OT requirements, rail transportation infrastructure presents a different set of security risk challenges compared to other large complex public infrastructure, and ultimately cybersecurity solutions need to be tailored to the specific characteristics of the industry. To be effective and reliable, a general rail transit security solution package must be planned, implemented and managed as an end-to-end holistic process and to this end, cybersecurity is a component within the general organizational security package [16, 17]. Some tactical-level guidelines/requirements for design, deployment and operation/maintenance of an effective cybersecurity safeguards and countermeasures mechanism for a typical rail transit system can be listed as:

1. *Security design to target a mission-critical application with crucial safety requirements [18, 19]*:

   a. Both security and safety are inversely proportional to risk. In other words, if it is not secure, it has a high degree of risk associated to it and it is unlikely to be safe.
   b. Security measures should be qualitatively and quantitatively proportional to corresponding threats, i.e., the residual risk to be rigorously and recursively assessed and verified.
   c. Saltzer-Schroeder's principles provide a solid base for cybersecurity design [20]. They include economy of mechanism, fail-safe defaults, complete mediation (every access to every object must be checked for authority), open design, separation of privilege (two keys are better than one), the least privilege, the least common mechanism, and psychological acceptability (design for ease of use).
   d. Cybersecurity safeguards and countermeasures should be foreseen and devised from the concept development (stage zero) onwards. This closely follows the principles of 'Shift Left' and 'Start Left', used in the software and application development domain, and aims to incorporate cybersecurity in to the product development process, right from the initial stages.
   e. An attack at a layer lower than a protection may be able to defeat the protection, even if the protection is perfectly implemented. Alternatively, a protection at a lower layer than an expected attack may be able to defeat the attack, even if the attack is expertly conducted.

2. *Multi-level cybersecurity plan*: Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect and identify potential attacks, respond in an appropriate manner, minimize the impacts, and recover from attacks. Therefore, three phases of an effective cybersecurity plan of action can be identified as:

    a. *Protect*: Install specific protection measures to prevent and discourage cyber-attacks.
    b. *Detect*: Establish mechanisms for rapidly identifying actual or suspected cyber-attacks.
    c. *Respond*: Undertake appropriate action in response to confirmed security incidents to achieve business continuity or disaster recovery.

3. *Importance of following lessons learned/best practices procedures:* To make technical, procedural, and managerial protection measures more efficient, it is essential that people operate best practices. Best practices procedures document needs to be periodically updated based on the lessons learned.

4. *Drive up difficulty*: Attackers can be defeated by driving the level of difficulty of technical protection measures beyond their ability to cope. Three considerations for analyzing difficulty are inherent system weakness, attacker access to the weakness, and attacker capability to exploit weakness [21]. Attacker capability is beyond the control of a protection specialist. Therefore, the two viable options for driving up difficulty are to reduce inherent system weakness and restrict availability to reduce attacker access.

5. *Defense in depth*: Security measures should be applied in series to avoid single points of failure. Where a single measure has been deployed to protect a system, there is a risk that if a weakness in that measure is identified and exploited, there is effectively no protection provided.

6. *Distract with Decoys/Divert attackers to other targets [22]:* Encouraging a false belief in success or frustration through using decoy targets (e.g., honeypots/tarpits) is a valid protection option. Furthermore, diverting attention to a more attractive target away from your protected assets is an effective strategy.

7. *Compliance strategy*: It is necessary that the dossier of evidence supporting a system's safety regulation compliance includes provisions for cybersecurity compliance. Security compliance requires initial certification/accreditation and periodic renewals through internal/external security audits.

8. *"System Engineering" approach to cybersecurity implementations [11]:*

    a. Security Concept of Operations (ConOPs) principles and requirements to involve people from start of project
    b. Systematic way to define, design, validate, implement, verify (test), and commission security requirements
    c. Mapping cybersecurity framework against V-model (i.e., the Software Design Life Cycle model where execution of design and verification processes happens in a sequential manner in a V-shape) to follow the approach of identify, protect, detect, respond, and recover through a systematic V-model approach

9. *Business-oriented industry-level security training*: Staff who interact with systems must be appropriately trained to comply with good security principles. Different aspects of security training include (depending on level and scope of knowledge required):

    a. General awareness of cybersecurity, this should be imparted to every member of the organization's staff, irrespective of their role and responsibilities.
    b. Understanding the core of problems and the interconnected nature of security and safety.
    c. Understanding the differences between mission-critical control systems and IT systems from a security point of view.
    d. The need to consider the whole life-cycle, not just deployment but also operations (impacts on ConOPs) and maintenance (impacts on Concept of Maintenance or ConMAIN).
    e. The ongoing and persistent requirement for vulnerability assessment/risk analysis (e.g., network vulnerability scanning and penetration testing) and vulnerability management (e.g., patching, Operating Systems, firmware, and application code)
    f. The importance of change management including multi-layer testing of equipment from manufacturer before it gets installed, system change issues, and system/network boundary awareness.
    g. Incorporating cyberattack scenarios in to the organization's emergency preparedness plans and operational training.

Concluding Remarks

Railway transportation communications networks include safety-critical infrastructure; therefore, the impact of potential cybersecurity incidents on the railway system can be significant. This calls for the need of a security concept to ensure the robustness and resilience of railway communications networks against cyberattacks. Cyber resiliency focuses on capabilities supporting organizational missions or business functions. Shifting from a purely system-hardening security focus to a comprehensive and flexible system prevention and recovery approach allows for efficient and dynamic allocation of resources. The first and foremost requirement for devising such a comprehensive and flexible cybersecurity framework is developing in-depth and holistic insights about rail transportation concepts of operations and proportional cybersecurity countermeasure technologies.

Most rail organizations have existing resilience features, methods, and requirements for responding to cybersecurity accidents and disaster conditions. These processes can be subjected to thorough risk/vulnerability assessment analyses, utilized wherever possible, and eventually expanded to provide a resilient and up-to-date cyber-defense mechanism. Reusing existing countermeasures and incorporating them in a holistic, integrated, and end-to-end cyber-defense framework is a reasonable initial approach to minimizing system security rework. The system, however, needs to be periodically re-evaluated to stay up-to-date with respect to the ever-evolving cyber-threat vector.

Rail transportation decision-makers need to realize cybersecurity involves a human dimension, which is as important as the technical aspect. Cybersecurity policies, practices, and training must extend to all elements of rail transportation including within transportation authorities as well as supporting vendors and third-party contractors whose lack of knowledge and preparation can prove equally disastrous for the organizations themselves.

References

1. P. Darlington, Advances in Railway Cybersecurity, RailEngineer (www.railengineer.co.uk), November 2018
2. B. Chen et al, Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective, Proc. Of Int. Conf. on Computer Safety, Reliability, and Security (SAFECOMP 2014, pp. 277-290), 2014
3. 2018 Annual Data Breach Year-end Review, Identity Theft Resource Center, January 2019 (https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf)
4. 2018 Study on Global Megatrends in Cybersecurity, Ponemon Institute, February 2018 (https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf)
5. By the Numbers: Global Cyber Risk Perception Survey, Marsh and Microsoft, February 2018 (https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html)
6. 2017 Trustwave Global Security Report, Trustwave Holdings Inc. (https://trustwave.azureedge.net/media/14701/2017-trustwave-global-security-report.pdf?rnd=131992184380000000)
7. 2019 Cost of A Data Breach Report, Ponemon Institute, Sponsored by IBM Security (https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf)
8. Koramis & Sophos, Whitepaper Project HoneyTrain, Technical Report, September 2015
9. A. Thaduri, M. Aljumaili, R. Kour, R. Karim, Cybersecurity for eMaintenance in Railway Infrastructure: Risks and Consequences, International Journal of System Assurance Engineering and Management (Springer), pp. 149-159, March 2019
10. Cybersecurity Considerations for Public Transit, APTA Recommended Practices (APTA SS-ECS-RP-001-14), Enterprise Cybersecurity Working Group, October 2014
11. APTA 2019 Rail Conference (Toronto) Track 4: 21st Century Security Concerns and Cybersecurity in Transit, Panelists: K. Oberle, A. W. Lee, C. Johnson
12. CYRail Recommendations on Cybersecurity of Rail Signaling and Communication Systems, Horizon 2020 European Union Funding for Research and Innovation (www.cyrail.eu), September 2018
13. Rail Cyber Security Strategy, National Rail's Rail Delivery Group (cyber-security@raildeliverygroup.com), January 2017
14. Rail Cyber Security: Guidance to Industry, Department for Transport (www.gov.uk/dft), 2016
15. S. Baruah, H. Li, and L. Stougie, Towards the Design of Certifiable Mixed- Criticality Systems, in Proceedings of the 16th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), pp. 13–22, 2010
16. A. G. Hessami, A Systems View of Railway Safety and Security, in Railway Research-Selected Topics on Development, Safety and Technology (Chapter 2), Publisher: InTech, 2015
17. H. Bock, J. Braband, B. Milius, and H. Schabe, Towards an IT Security Protection Profile for Safety-Related Communication in Railway Automation, Computer Safety, Reliability, and Security (Springer), pp. 137–148, 2012
18. J. Braband, Towards an IT Security Risk Assessment Framework for Railway Automation, CoRR abs/1704.01175, http://arxiv.org/abs/1704.01175, 2017
19. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, A Survey of Approaches Combining Safety and Security for Industrial Control Systems, Reliability Engineering & System Safety, vol. 139, pp. 156–178, 2015

20. R. E. Smith, A Contemporary Look at Saltzer and Schroeder’s 1975 design principles, IEEE Security and Privacy, Vol. 10, Issue 6, pp. 20-25, 2012
21. J. Hughes and G. Cybenko, Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity, Tech. Innovation Manage. Rev., pp. 15-24, Aug. 2013
22. K. S. Wilson and M. A. Kiy, Some Fundamental Cybersecurity Concepts, IEEE Access, Vol. 2, pp. 116-124, 2014