CYLUS

The Rail Cybersecurity Landscape in 2025

A defining year for rail cyber maturity and operational resilience

Contents

Executive Snapshot

In 2025, rail cybersecurity is increasingly focused on operational outcomes, service continuity, recoverability, and the ability to contain disruption, rather than on the number of policies or tools an organization has. Two forces are accelerating this shift: (1) rail-specific engineering guidance that integrates cybersecurity into lifecycle thinking, and (2) a steady rise in publicly visible disruptions and disclosures that make rail cyber risk harder to treat as "background."

Across regions, maturity is less about having policies and more about whether controls are repeatable and evidenced in live OT environments. The industry's technical center of gravity is converging around a practical operating model: visibility (asset truth and data-flow understanding), defensible architecture (segmentation aligned to rail boundaries and controlled remote/supplier access), and lifecycle assurance. In Europe, the direction set in 2023 reinforced cybersecurity by explicitly aligning cybersecurity with the EN 50126-1 RAMS lifecycle and grounding risk concepts in IEC/EN 62443.

At the same time, ENISA's rail guidance operationalizes zoning and interdependency thinking. Internationally, IEC 63452 is emerging as a unifying rail cybersecurity reference, building on CLC/TS 50701 and IEC 62443 concepts and setting expectations for more consistent, lifecycle-driven assurance across markets as it approaches publication.

What 2025 cyber incidents continue to demonstrate is that rail impact often shows up first within the operational environment itself: systems that enable dispatch and service coordination, operational communications, passenger information, control-room visibility, and supplier-connected support platforms that sit on the OT boundary. When these are disrupted, the effects are immediate and operational: degraded situational awareness, slower decision loops, manual procedures, and reduced control over service delivery and recovery, creating a real risk to service continuity across the industry.

Heading into 2026, the operators pulling ahead are those treating cybersecurity as a routine, cross-functional operating rhythm: maintaining OT inventories and taxonomy, segmentation, and remote access that match real rail boundaries, vulnerability, and configuration processes that respect safety/change constraints, and exercised detection/response and recovery that are coordinated with engineering, operations, and key suppliers. Investment priorities follow the same logic: funding capabilities that improve control, visibility, and recoverability, aligned with ongoing operational requirements rather than one-time transformation projects.

1. Where Operators Stand in 2025: Maturity and Investment Snapshot

In 2025, rail cybersecurity is increasingly being integrated into engineering, operations, and service-continuity management, rather than treated solely as a corporate IT function. This shift is not uniform globally, but it is driven by regulatory pressure, intensifying threat-actor activity, and critical-infrastructure oversight frameworks that increasingly require evidence of cyber-risk management within operational environments.

In the European Union, this integration is reinforced by both regulation (NIS2) and rail-specific engineering guidance (CLC/TS 50701), which links cybersecurity activities to established assurance and lifecycle processes (European Union, 2022; CENELEC, 2023).

At the international level, IEC 63452 (Railway applications - Cybersecurity) is under development to provide a rail-specific, internationally aligned reference, with publication expected in 2026, subject to IEC voting and publication steps (IEC, 2025).

ENISA's Railway Cybersecurity – Good Practices in Cyber Risk Management continues to serve as a baseline reference in Europe, emphasizing that cyber risk management for railways must be adapted to operational constraints, safety considerations, and system lifecycles rather than applied as generic IT control checklists (ENISA, 2021).

In the United States, rail cybersecurity maturity in 2025 is shaped less by rail-specific engineering standards and more by federal oversight and risk-management expectations for critical infrastructure. The Transportation Security Administration's 2024 Notice of Proposed Rulemaking on surface transportation cybersecurity signals a move toward formalized requirements for cyber risk management, incident reporting, and resilience for covered rail operators. (TSA, 2024).

Across the Asia-Pacific region, maturity remains uneven and is primarily driven by national critical-infrastructure regimes rather than rail-specific cybersecurity standards.

We've seen Australia and Singapore strengthen mandatory cyber-risk management, incident-reporting, and resilience obligations for transport operators by updating their critical infrastructure and cybersecurity legislation. At the same time, large metro and mainline programs continue to rely heavily on vendors and system integrators. In this context, operators typically align technical controls with IEC 62443 concepts and national cybersecurity frameworks, with rail-specific guidance influencing procurement and assurance practices for major modernization projects (Australian Government, 2024; Singapore Statutes Online, 2024; UITP, 2025).

Across regions, maturity in 2025 is less about the existence of policies and more about whether controls are repeatable and evidenced in live OT environments. Higher-maturity operators can typically demonstrate:

- Authoritative OT asset inventories and network/data-flow representations, enforced segmentation and controlled remote access, including supplier access
- Vulnerability identification and remediation processes that operate within safety, availability, and change-control constraints
- Monitoring, incident response, and recovery capabilities that are exercised and coordinated across internal teams and key suppliers

(NIST, 2024; Rail Delivery Group, 2025).

Investment priorities in 2025 increasingly reflect this operational view of maturity. Rather than isolated modernization projects, operators are directing resources toward capabilities that improve control, visibility, and recoverability in operational environments, such as secure remote access, segmentation aligned with safety-critical boundaries, vulnerability and configuration management under operational constraints, OT detection and monitoring, and tested resilience and recovery planning. Sector-level strategies continue to note that preparedness and protection remain inconsistent across rail ecosystems, reinforcing the need to treat cybersecurity as an ongoing operational requirement rather than a one-time transformation effort (Rail Delivery Group, 2025).

Taken together, these developments set the stage for 2026: a period in which cybersecurity is increasingly expected to function not as a collection of discrete projects, but as a routine element of engineering assurance, operational governance, and service continuity management across the rail sector.

2. Strategic Cyber Trends Shaping Rail

Rail cybersecurity is shifting from a “specialist topic” to an operational requirement. Standards are converging, regulation is moving into enforcement, and real-world incidents and advisories are making cyber risk tangible across signaling, rolling stock, communications, and supporting OT.

This section is a high-level map of the trends shaping rail cybersecurity in 2025. The detailed analysis appears later in this document: frameworks and standards (Section 4), regulation (Section 5), attacks (Section 6), notable vulnerabilities/advisories (Section 7), and the operator playbook (Section 8).

2.1 Global Rail Cyber Standards Move Toward a Common Ground

Rail cybersecurity standards are starting to “fit together” into a shared language. CLC/TS 50701 provides rail-specific guidance aligned with rail lifecycle practices, while IEC 62443 supplies a widely adopted control structure and assurance model. IEC 63452 is expected to consolidate this direction into a globally consistent rail cybersecurity standard.

What this means in practice: operators and suppliers can increasingly align on common concepts (zones and conduits, security levels, lifecycle assurance, and evidence-based requirements), even when implementation varies by region or operator (ENISA, 2022). For the full framework breakdown and how the pieces relate, see Section 4.

The market is moving toward clearer expectations for “what good looks like” across design, integration, operations, and supplier assurance, reducing ambiguity for procurement and assessments over time.

IEC 63452 Timeline

August 2025 - October 2025
National committees review

- Draft circulated to national committees
- Comments collected on terminology, zoning, lifecycle alignment, and consistency with IEC 62443

September 2025 – March 2026
Final Draft International Standard (FDIS)

- Technical adjustments made ahead of the final vote

March – May 2026
Final Draft International Standard (FDIS) vote

- IEC submits IEC 63452 for the FDIS vote
- Double vote expected, as international IEC, but also as European CENELEC EN
- Content is effectively final at this stage
- Approval at FDIS authorizes publication

Mid-2026
Publication

- IEC 63452 published as a full International Standard
- Becomes the first globally recognized cybersecurity standard explicitly written for rail

2.2 Regulation Moves Into Enforcement

Across major markets, rail cybersecurity regulation is shifting from guidance to enforceable obligations. The result is less tolerance for informal programs and more demand for demonstrable governance, reporting, and supply-chain assurance.

- In Europe, NIS2 strengthens supervisory expectations and incident reporting, while the Cyber Resilience Act raises the bar for security of connected products and software in the supply chain (European Union, 2024). In the United States, TSA rail cybersecurity requirements continue to mature toward more formalized expectations (Transportation Security Administration, 2024).
- For operators, the practical impact is that cybersecurity is increasingly reflected in procurement language, contractual obligations, audit readiness, and executive accountability, not just technical controls.

For a detailed regulatory breakdown by regime and its implications for rail stakeholders, see Section 5.

2.3 Rail Becomes a Strategic Asset in Geopolitical and Military Mobility Contexts

Railway systems have become strategically significant as geopolitical tensions increasingly extend into critical infrastructure. Rail supports not only civilian transport and commercial logistics but also military mobility and defense readiness. EU-level policy work on military mobility explicitly references enabling more flexible rail vehicle operation and enhancing protective measures for dual-use infrastructure (European Union, 2025).

Rail is also increasingly treated as a high-impact target category within transport cyber threat analysis. ENISA's transport threat landscape work analyzed attacks across transport modes (including rail) and highlights how digitization and criticality increase systemic impact (ENISA, 2023).

These developments illustrate how rail is no longer a peripheral asset in cyber or hybrid warfare. Its role in enabling civilian mobility, commercial logistics, and military transport makes it a rising strategic target. Ensuring visibility and resilience across OT and IT layers becomes critical to preserving operational continuity under both civilian and defense demands.

For examples of how this plays out in real incidents and adversary intent, see Section 6.

2.4 Vulnerability Disclosure Becomes Standard

Historically, rail-cyber vulnerabilities were rarely publicly disclosed due to safety sensitivities and legacy security cultures. That pattern is changing. More vendors and researchers are publishing advisories, and more operators are expected to act on them quickly and consistently.

The operational requirement is an intake and triage process that can translate advisories into action: asset impact determination, compensating controls, patch planning, and supplier follow-up, without disrupting safety-critical operations.

For notable advisories and recurring patterns relevant to rail environments, see Section 7.

2.5 Visibility Becomes the Core of Cyber Operations

Visibility is becoming the core of rail cyber operations because every other capability depends on it: segmentation, monitoring, incident response, and evidence for compliance.

In practical terms, operators are prioritizing asset inventory, communications mapping, and "how the system really behaves" across interconnected OT and IT domains. This also supports system-level design approaches such as zones and conduits.

For how mature operators operationalize visibility (and why it is the starting point of a pragmatic program), see Section 8.1.

2.6 AI Begins to Influence Rail Cyber Operations and System Behavior

AI is increasingly influencing how both operators and adversaries interact with rail systems. Although its adoption across rail OT remains early, several clear patterns are emerging. Operators are using AI to support condition-based maintenance, network monitoring, and operational planning. At the same time, the broader cybersecurity ecosystem is seeing the rise of models that lower the technical threshold for intrusive activity, automate reconnaissance, and generate more convincing social engineering attempts (National Cyber Security Centre, 2024).

For rail, the impact is practical. AI accelerates the interpretation of operational data, but it also increases the volume of data that must be understood in context. It is increasingly important to distinguish among regular shifts in system behavior, maintenance activities, misconfigurations, and malicious intent. Rail environments that rely on legacy assets, vendor-specific logic, and distributed architectures require visibility to validate or challenge AI-generated insights (McKinsey & Company, 2024).

When deploying AI systems (including externally developed tools), government guidance emphasizes secure deployment practices and governance to avoid introducing new vulnerabilities and data risks (CISA, 2024).

3. The Industry Forums Defining Rail Cybersecurity

The evolution of rail cybersecurity has been shaped primarily by industry forums, technical alliances, and policy bodies in which operators, OEMs, regulators, and suppliers convene to define the sector's priorities. Long before requirements are formalized or legislation is drafted, these groups are where rail organizations surface shared challenges, compare operational realities, and build a collective understanding of what "secure rail" entails.

In these settings, cybersecurity ceases to be an isolated technical issue and becomes a system-level concern linked to safety, reliability, digital modernization, and cross-border interoperability. The discussions, guidance, and technical work produced in these groups lay the groundwork for everything that follows, informing future engineering frameworks, procurement expectations, and ultimately, regulatory direction.

Below are some of the most influential bodies shaping the global rail cybersecurity agenda.

3.1 Europe's Rail Joint Undertaking / ERJU

Europe's Rail Joint Undertaking (EU-Rail/ERJU) is a cornerstone of Europe's collaborative approach to modernizing railway systems under Horizon Europe, established by Council Regulation (EU) 2021/2085 (ERJU, 2021).

Through its System Pillar, EU-Rail acts as a sector-level "system integrator," developing a unified operational concept and a functional, safe, and secure system architecture for an interoperable European railway system (ERJU, 2021).

ERJU's cross-pillar collaboration has also been instrumental in harmonizing safety and cybersecurity certification models, helping bridge the gap between CENELEC standards (such as CLC/TS 50701) and on-the-ground operational realities. The initiative provides a blueprint for integrating cybersecurity into complex modernization projects, ensuring that European railways remain both interoperable and defensible by design.

The European Rail Joint Undertaking (EU-Rail) published the Cybersecurity Specification V1.0 in March 2025 to enable interoperability of cybersecurity interfaces across European rail automation systems (ERJU, 2025). The specification supports compliance with key EU cybersecurity regulations, including NIS2, CRA, CSA, and RED, while aligning with international standards such as ISO 27001, IEC 62443, and CLC/TS 50701. It is structured around main specifications covering:

- Secure components
- Secure communications
- Shared cybersecurity services and organizational cybersecurity processes

Together, these define technical, communication, service-level, and governance requirements that ensure consistent cybersecurity implementation across the rail sector. The specification is supported by additional documents addressing regulatory traceability, risk assessment, threat modeling, and product documentation. Endorsed by both industry and railway operators, it is expected to significantly reduce operator-specific security requirements and foster a more interoperable and efficient European rail cybersecurity market (ERJU, 2025).

3.2 Union des Industries Ferroviaires Européennes / UNIFE

UNIFE (Union des Industries Ferroviaires Européennes) represents the European rail supply industry and engages in digitalization and cybersecurity through dedicated committees and working groups (UNIFE, 2025).

UNIFE's cybersecurity task forces and technical committees play a crucial role in interpreting evolving EU legislation, including the NIS2, the Cyber Resilience Act (CRA), and the Radio Equipment Directive (RED), for the rail sector. The association has emphasized secure development lifecycle practices and transparency in Software Bill of Materials (SBOMs), recognizing that supplier accountability is essential in the era of connected, software-defined rail systems.

In 2025, UNIFE's Cybersecurity Working Group intensified its collaboration with both the European Committee for Electrotechnical Standardization (CENELEC) and the European Union Agency for Railways (ERA) to develop a more precise definition of "cybersecurity assurance" for supplier certification. Its position papers and industry consultations now serve as a predictive lens for upcoming regulatory shifts, helping the rail ecosystem prepare for new procurement and compliance realities (UNIFE, 2025).

3.3 American Public Transportation Association / APTA

In North America, the American Public Transportation Association (APTA) has become a key forum bridging the gap between cybersecurity theory and operational practice in transit and commuter rail systems. Supported by the Federal Transit Administration (FTA) and in alignment with the Transportation Security Administration (TSA) Security Directives, APTA's working groups have moved cybersecurity from a niche IT topic to a core element of the transit safety conversation.

Recent initiatives within APTA's Rail Transit Committee and Cybersecurity Working Group have focused on OT asset management frameworks, incident coordination playbooks, and AI oversight for predictive maintenance and autonomous systems. Their outputs, such as best-practice guides and peer-exchange programs, are increasingly referenced by agencies implementing TSA directives or pursuing compliance with NIST and IEC frameworks (APTA, 2025).

3.4 North America Transit Cybersecurity Consortium

For North American rail operators, alignment of rail and transit cybersecurity is increasingly shaped by the North America Transit Cybersecurity Consortium. This MTA-hosted forum convenes public transportation entities, critical infrastructure partners, regulators, and policymakers to share operational lessons and advance practical cybersecurity priorities.

Complementing the forum, the consortium produces implementation-focused artifacts, most notably its OT Procurement Requirements guidance, intended as a baseline for transit agencies, integrators, and suppliers, and aligned with widely used frameworks such as IEC 62443 and NIST SP 800-82 (NACITCC).

3.5 Union Internationale des Transports Publics / UITP

The Union Internationale des Transports Publics, or International Association of Public Transport (UITP), serves as a global bridge for cybersecurity dialogue, connecting metros, light rail operators, and mobility authorities across continents.

UITP has produced practical cybersecurity guidance tailored to public transport tendering/procurement, explicitly framing cybersecurity as a growing, cross-functional concern in public transport and railways (UITP, 2023).

UITP also publishes (member-access) guidance on cybersecurity risk assessment approaches for public transport operators, reflecting the sector's need to translate governance into implementable practices (UITP, 2025).

UITP is about to publish a thorough document guiding how to approach cybersecurity for safety instrumented systems. The document is already in the final review and editorial polishing state.

4. The Frameworks Defining Rail Cybersecurity

Entering 2026, rail cybersecurity standards are no longer just "technical requirements," they are reshaping accountability by pushing the industry toward evidence-based assurance rather than checklist compliance. In rail, this means safety, reliability, and cybersecurity are increasingly managed as interdependent properties of a single system across the full lifecycle, rather than as separate disciplines with separate proof (ERA-ENISA, 2023).

4.1 CENELEC CLC/TS 50701 (Railway Applications — Cybersecurity)

Since its first publication in 2021, CENELEC TS 50701 has become the worldwide reference framework for rail cybersecurity. The 2023 second edition tightened alignment with IEC 62443 and EN 50126, embedding cybersecurity into the same lifecycle principles that govern safety and reliability. Its adoption is widespread among European operators and OEMs, with growing recognition in the Asia-Pacific and the Middle East. While IEC 63452 will eventually replace it, TS 50701 remains the benchmark for "good" practice, demonstrating that safety engineering and cybersecurity can coexist (CEN-CENELEC, 2023).

4.2 IEC 63452 (Railway Cybersecurity – forthcoming International Standard)

IEC 63452 is being developed as an international rail cybersecurity standard under IEC, aimed at providing a consistent rail-specific approach that builds on established rail cybersecurity and lifecycle concepts. Building on the foundation of CLC/TS 50701 and, the IEC 62443, this new IEC specification seeks to consolidate the fragmented approaches across Europe, North America, and Asia into a single framework. The drafting process, now deep in committee, reflects a significant shift: cybersecurity is no longer a national conversation but a global one. Once finalized, IEC 63452 is expected to define how cybersecurity requirements are expressed in contracts, certifications, and operational assurance (IEC, 2025).

4.3 IEC 62443 (Industrial Automation and Control Systems Security)

IEC 62443 is a globally recognized series for securing industrial automation and control systems (IACS), defining requirements and processes for implementing and maintaining security across OT environments (ISA, 2021). In the rail context, it functions as the underlying cybersecurity "control language" and structure that rail-specific standards (like CLC/TS 50701 and the IEC 63452 work) draw from and align with.

5. Regulations to Watch

Rail cybersecurity has entered its enforcement era: the conversation has shifted from voluntary frameworks toward binding legal obligations that can drive both organizational governance and technical outcomes. Across major markets, regulators are moving beyond recommending best practices to defining minimum requirements for how critical infrastructure entities manage risk, respond to incidents, and engineer digital systems to be secure by design.

What makes the current landscape particularly complex and consequential is the interplay between horizontal legislation that applies across sectors and vertical, transport-specific obligations that tailor or amplify those expectations for rail. As these regulatory authorities take effect, rail operators and suppliers must reconcile multiple layers of legal compliance with engineering and assurance practices, effectively making cybersecurity a standard feature of regulated infrastructure governance rather than a voluntary add-on.

5.1. NIS2 (EU) - Horizontal Framework for Critical Sectors

NIS2 applies to entities in high-criticality sectors, including transport, and explicitly includes railway undertakings in Annex I. It sets cybersecurity risk-management expectations and incident-reporting obligations, including an "early warning" within 24 hours of becoming aware of a significant incident. Member States' transposition deadline was October 17th, 2024, though implementation maturity varies by country (European Union, 2022).

5.2 Cyber Resilience Act (EU) - Product-Centric and Supplier-Heavy

The CRA is Regulation (EU) 2024/2847 and introduces EU-wide cybersecurity requirements for "products with digital elements," including vulnerability handling, reporting pathways, and documentation expectations. It takes effect on December 11, 2027, with earlier application dates for specific parts (e.g., certain reporting obligations from September 2026 and notified body provisions from June 2026).

The CRA also defines and references the concept of a software bill of materials (SBOM) and enables authorities to request SBOM information as needed for compliance checks (European Union, 2024).

5.3 TSA Surface Cyber NPRM (U.S.) - Vertical Regulation for Surface Transport

In the United States, the Transportation Security Administration (TSA) is codifying what began as temporary directives into permanent regulations. Its Surface Cybersecurity NPRM, released in November 2024, introduces enforceable obligations for freight and passenger railroads, pipelines, and transit agencies.

The proposal instructs 24-hour incident reporting, risk management plans, and supply-chain oversight - effectively placing rail cybersecurity under the same regulatory gravity as aviation and energy. In partnership with CISA, TSA's framework signals a broader U.S. strategy: treating cybersecurity as critical-infrastructure management, not merely IT governance (TSA, 2024).

5.4 ERA / ERJU Cyber Programs - Vertical Enforcement through System Integration (EU)

The European Union Agency for Railways (ERA) and Europe's Rail Joint Undertaking (ERJU) now act as the operational arm of EU cyber policy. Their joint initiatives translate legal obligations, such as those under NIS2 and the CRA, into technical and certification criteria for ERTMS and EULYNX. In practice, these programs ensure that funding eligibility, innovation grants, and system certifications are tied to cybersecurity baselines. By 2026, participation in ERA and ERJU cyber programs will determine whether organizations are compliant with Europe's digital rail agenda or excluded from it (ERA, 2025).

Category	Name	Primary Purpose	Scope	What Matters Most
Standard	IEC 63452	Unified global cybersecurity framework for rail	Entire rail system lifecycle, including Signaling, rolling stock, telecom, control centers, etc	International harmonization; Alignment with EN 50126 & IEC 62443
Standard	CLC/TS 50701	European cybersecurity framework for rail	Entire rail system lifecycle, including Signaling, rolling stock, telecom, control centers, etc	Alignment with EN 50126 & IEC 62443. Will be overseen by IEC 63452.
Standard	IEC 62443	Foundational industrial cybersecurity framework for OT environments	All industrial control systems, including signaling, rolling stock, telecom, and control centers	Defines lifecycle, zones/conduits, and SL, the foundation for CLC/TS 50701 and IEC 63452
Regulation	NIS2 (EU)	Mandatory cybersecurity for European critical infrastructures and essential services	Rail operators & infrastructure managers	Risk mgmt., incident reporting, supply-chain obligations
Regulation	Cyber Resilience Act (EU)	Product security requirements	Suppliers of digital components	secure-by-design, vulnerability handling
Regulation	TSA NPRM (U.S.)	Operational cybersecurity oversight	Freight/passenger rail & transit	24-hour reporting; risk mgmt.; operational resilience
Regulation/ Program	ERA/ERJU Programs (EU)	Enforcement of cyber baselines via system engineering	ERTMS, EULYNX, digital rail upgrades	Interoperability and technical compliance

6. State of Rail Cyber Attacks

2025 is a good “reality check” year for rail cyber risk because it shows (a) how quickly rail service can be disrupted through IT-facing systems, and (b) how often rail impact arrives through third parties, even when safety-critical operations continue to run. Significantly, most of what we can analyze publicly is still based on disclosed incidents, so any trend lines should be framed as “publicly reported incidents,” not total incident volume.

ENISA’s transport threat landscape (covering Jan 2021–Oct 2022) logged 98 publicly reported transport incidents, including 21 railway incidents. This serves as a baseline, showing that rail is consistently visible in transport cyber reporting and is most commonly affected by ransomware, data-related threats, and denial-of-service patterns seen across the sector (ENISA Transport Threat Landscape, 2023).

6.1 Notable 2025 Cases

The following examples of publicly reported incidents in 2025 illustrate the diversity of impacts rail operators are managing today.

6.1.1 PKP Intercity (January 2025)

Polish media reported that PKP Intercity experienced a cyberattack-driven failure of its ticket sales system overnight in January 2025, causing problems purchasing tickets through electronic channels, with similar electronic-access issues recurring in early February. Reporting noted that passengers could still buy tickets at staffed ticket offices and, in some cases, via external apps, meaning the disruption primarily affected digital customer access while increasing reliance on in-person operational processes at stations (Polskie Radio, 2025).

6.1.2 Ukrzaliznytsia (March 2025)

Reuters reported that Ukrzaliznytsia suffered a major cyber attack that disrupted its online systems, including online freight services, leading the railway to switch to paper-based systems and issue procedural updates for commercial customers (including wagon orders/dispatches). While public statements emphasized that train operations continued, the incident still affected the operational execution layer around freight (how movements are requested, coordinated, and processed day-to-day), which can translate into real operational friction even when control systems are not reported as impacted (Reuters, 2025).

6.1.3 Maryland Transit Administration (August 2025)

MTA Maryland reported a cybersecurity incident involving unauthorized access to certain systems. Official updates described impacts on rail signage/digital screens, as well as on systems that typically provide real-time rail information. Local reporting also stated that Mobility paratransit was unable to schedule new trips or rebook existing trips, and that riders would not see station notifications for train arrivals/departures, a clear example of an incident that doesn't stop trains but degrades operational visibility and operational support functions (information, scheduling, coordination) (Maryland Transit Administration, 2025).

6.2 What 2025 Shows More Clearly Than Prior Years

Across the rail stories that surfaced publicly in 2025, some patterns stand out:

1. 2025 reinforces that rail cyber risk is fundamentally an OT problem, because the most successful disruptions targeted the technology that runs the railway as a physical system: operational visibility, service coordination, dispatch, freight execution workflows, and the passenger-information layer that regulates station flow and recovery actions. These are not "just IT apps"; they are operational technologies that sit within the rail operational environment and directly shape throughput, punctuality, and the ability to manage disruptions safely. When these systems are degraded, operators lose real-time awareness and coordinated control of service delivery, forcing manual modes (paper-based freight processes, manual rebooking, and degraded real-time visibility). That shift is the clearest OT impact: reduced operational control, slower decision loops, higher workload, and a greater likelihood of cascading delays as the railway moves from instrumented operation to human-driven fallback.
2. Rail's strategic infrastructure framing continues to raise attacker interest and public visibility. The Ukrzaliznytsia case in particular was reported in a geopolitical context. It included disruptions to freight-facing services, underscoring that rail is treated as strategic infrastructure and that cyber incidents can target the operational execution environment, even without publicly reported effects on signaling.

6.3 Who Targets Rail, and What They Are Trying to Achieve

Public reporting and sector-level analyses identify three recurring "actor clusters" targeting rail and the broader transportation sector. The key point for rail is that these actors typically target the most operationally leveraged digital surfaces, public services, supplier dependencies, and operations-facing coordination systems, because disrupting coordination is often easier (and more visible) than directly compromising safety-critical control systems (ENISA, 2023).

6.3.1 Cybercriminal ecosystems

- Who they are: financially motivated groups (often operating as Ransomware-as-a-Service, with affiliates).
- What they want: money (encryption + extortion via data theft), sometimes "double/triple extortion."
- Where they hit rail: enterprise IT, third-party services, identity systems, and "operationally important" business platforms (e.g., portals, scheduling, customer comms) that cause the most significant disruption and pressure.

Rail is not targeted only by "rail-specialist" groups; it's targeted by scalable ransomware ecosystems that hit many critical-infrastructure sectors, including transportation (CISA, 2023).

6.3.2 Hacktivists and ideologically motivated groups

- Who they are: politically motivated collectives, often volunteer-based, frequently operating in waves around geopolitical events.
- What they want: visibility, signaling, and disruption.
- What they hit rail: most commonly, DDoS attacks against services.

A concrete rail example is the Poland “radio-stop” incident (August, 2023) when unauthorized actors broadcast the “radio-stop” command over rail VHF, triggering emergency braking and halting 20+ passenger and freight trains. Reporting noted the broadcasts included pro-Russian audio (e.g., the Russian anthem / Putin speech excerpts), and Polish authorities investigated the event in a geopolitical context (AP News, 2023).

6.3.3 State-nexus actors

- Who they are: state-linked or state-aligned groups (sometimes blended with proxies).
- What they want: prepositioning, espionage, and, under some conditions, disruption aligned to geopolitical objectives.
- Where they hit rail: less via clean public attribution to a named unit, and more as a persistent strategic framing: transport is treated as national infrastructure, which increases attention, pressure, and the likelihood that rail incidents become publicly salient.

ENISA’s broader threat landscape explicitly tracks state-nexus activity as one of the major actor categories shaping overall risk (ENISA, 2024).

7. Notable Vulnerabilities & Security Advisories (2024–2025)

Public disclosures throughout 2024–2025 indicate a notable shift in the rail sector. Historically, vulnerabilities affecting railway systems were rarely published, with suppliers and operators generally avoiding open disclosure due to safety culture, national security sensitivities, and the absence of sector-specific reporting frameworks. In contrast, the past two years have seen a measurable increase in rail-relevant advisories issued through CISA, CERT@VDE, and vendor channels. These disclosures, spanning diagnostic platforms, wireless communication links, and industrial components, demonstrate how coordinated vulnerability reporting is becoming normalized in rail and highlight the growing operational significance of supply-chain exposure within complex, mixed-vendor environments.

7.1 HOT/EOT Freight Rail Radio Link Weak Authentication (CVE-2025-1727)

In 2025, CISA disclosed a weakness in the End-of-Train/Head-of-Train (EoT/HoT) remote linking protocol (CVE-2025-1727). CISA’s advisory explains that the protocol relies on a checksum rather than true authentication and that an attacker within RF range could craft packets (e.g., via software-defined radio) and issue brake-control commands to the EoT device, potentially causing disruption (CISA, 2025).

Importantly, Siemens Mobility’s Trainguard bulletin frames this as a protocol-level vulnerability and states that no software fix is currently planned for existing devices, reinforcing that some rail vulnerabilities require long-horizon mitigation (replacement protocols/equipment and layered compensating controls) (Siemens, 2025).

7.2 Frauscher Diagnostic System Vulnerabilities (CERT@VDE)

CERT@VDE advisories issued in 2025, including VDE-2025-030, reported OS command injection and access-control weaknesses in the Frauscher Diagnostic System (FDS). Although the axle counter system itself was not affected, the findings underscored the exposure introduced by connected diagnostic and maintenance platforms and the importance of segmentation and restricted access (VDE, 2025).

7.3 Examples of 2024 - 2025 Advisory Patterns Across Rail-Relevant OT Components

Across 2024–2025, rail-relevant vulnerability reporting increasingly reflected the reality of modern rail OT: much of the exposure lies in the industrial components that underpin rail architectures - routers, switches, secure remote access, protocol services, and embedded management planes. A steady cadence of disclosures through vendor PSIRTs and CISA's ICS advisory pipeline reinforced that this is now an ongoing operational lifecycle rather than an occasional event (CISA, 2025).

One clear example came from CISA, which published an advisory on Siemens SIMATIC ET 200SP communication processors, including SIPLUS "TX RAIL" variants, describing missing authentication for critical configuration connections (CVE-2025-40771). This is a good example of "rail OT exposure" emerging in the configuration/engineering surface—not only in signaling logic itself (CISA, 2025).

A related signal of ecosystem-wide exposure appeared in identity and access plumbing. Siemens ProductCERT documented that the RADIUS protocol issue known as "Blast-RADIUS" (CVE-2024-3596) impacts SCALANCE/RUGGEDCOM and associated products. In mixed-vendor OT, this matters because identity/auth decisions can undermine trust between network devices and authentication servers, turning "network plumbing" into a security-control-plane risk (Siemens Cert Portal, 2024).

Recent RUGGEDCOM disclosures also highlight how "everyday services" in network appliances can become a privileged compromise path. CVE-2024-56835 describes a code-injection risk via the DHCP server configuration file in RUGGEDCOM ROX II (versions < 2.17.0), where exploitation could enable a reverse shell and root-level access on the affected device (NIST, 2025).

Similar patterns show up across other widely deployed OT vendors. Moxa published advisories, including CVE-2024-9404, affecting multiple industrial switch families (DoS/system-crash risk), and separate 2025 advisories covering authorization/authentication weaknesses in network security appliances and routers. These are not rail-only products, but they are highly representative of the rail OT supply chain reality, where general-purpose industrial components can drive real operational risk if exposed or poorly segmented (Moxa, 2024).

CISA also published advisories for Westermo WeOS 5 that address an OS command-injection issue and an IPsec-related DoS scenario, illustrating how rail and other critical infrastructure operators inherit risk from embedded operating environments and secure tunneling stacks commonly used in field networking (CISA, 2025).

As a result, operators increasingly use CISA's ICS advisory stream and prioritization inputs, such as the Known Exploited Vulnerabilities (KEV) catalog, to triage patching and compensating controls across diverse assets - an approach that becomes increasingly critical as component-level advisories accumulate across mixed-vendor OT estates (CISA).

7.4 Context for the 2026 Landscape

The disclosures observed in 2024–2025 reinforce several shifts already outlined in this report. First, vulnerabilities are increasingly emerging in supporting and adjacent systems, diagnostics, wireless links, and embedded controllers, rather than only in core signaling or train-control domains.

Second, coordinated disclosure is maturing, with suppliers and CERT organizations adopting more structured reporting processes than in previous years. Third, the breadth of affected components underscores that supply-chain exposure has become a continuous operational concern, particularly in mixed-vendor environments where interdependencies are not always visible through traditional asset inventories.

Finally, the advisory patterns highlight the need for rail-contextualized visibility to determine where vulnerabilities reside, how they interact with safety-relevant systems, and which mitigations carry operational priority.

Taken together, the 2024–2025 advisory cycle illustrates how vulnerability management has evolved into a core element of the rail cybersecurity lifecycle, directly supporting the visibility, assurance, and governance expectations described above.

8. What Good Looks Like in 2026: The Operator Playbook

By 2026, “good” rail cybersecurity is less about accumulating controls and more about running a repeatable engineering-and-operations discipline: knowing what exists, knowing what depends on what, and being able to contain impact when disruption happens. Rail-specific frameworks are pushing the industry toward lifecycle assurance and evidence, not checkbox security (see Sections 2.1 and 4).

In practice, that means two capabilities become foundational. First: asset truth, a maintained OT asset inventory and taxonomy, because a “modern defensible architecture” depends on it (CISA, 2025). Second: architectural boundaries, clear segmentation of systems, and controlled interconnections, so issues in one area don’t automatically propagate across the railway. ENISA’s rail-specific Zoning and Conduits guidance is explicitly written to help operators do exactly this, based on CLC/TS 50701 (ENISA, 2022).

Against that backdrop, the ongoing IEC work on IEC 63452 signals a move toward a more consistent global rail cybersecurity playbook, but the operational core remains the same: lifecycle discipline, visibility grounded in reality, and architecture that limits blast radius.

8.1 Visibility as the Operational Backbone

The most consistent maturity marker is that operators can account for what exists, what connects to what, and what “normal” looks like in rail terms, not just IP addresses and servers. This is why modern OT guidance starts with asset inventory discipline: without a maintained inventory and taxonomy, risk decisions, vulnerability response, and incident handling collapse into guesswork (CISA, 2025).

In rail specifically, visibility is also the prerequisite for defensible segmentation. The zones-and-conduits approach (rooted in IEC 62443 concepts) assumes the operator can map functions, boundaries, and interdependencies well enough to decide what must be isolated, what must communicate, and under what conditions. ENISA’s rail-focused zones/conduits guidance explicitly aligns with CLC/TS 50701 in the rail context (ENISA, 2022).

This visibility-first approach is echoed and expanded in rail-specific guidance from the American Public Transportation Association (APTA). In its 2025 white paper, APTA frames visibility as a foundational operational capability rather than a discrete cybersecurity control. Visibility is defined not simply as asset awareness, but as a dynamic understanding of assets, data flows, system interdependencies, and interfaces across IT and OT environments. APTA explicitly distinguishes visibility from downstream practices such as detection, segmentation, or monitoring, emphasizing that without a shared, accurate view of what exists and how systems interact, these controls cannot be effectively designed, operated, or validated (APTA, 2025).

What “good” looks like in practice (evidence that an operator can produce):

- A maintained OT/rail asset inventory and taxonomy tied to safety-relevant functions and owners not a one-time spreadsheet).
- A zone/conduit model that reflects authentic operational architecture and vendor boundaries (not an IT network diagram).
- A visibility-driven operating rhythm (engineering + operations + cyber) that keeps the model current through change, maintenance, and upgrades (APTA, 2025).

8.2 Standards Embedded into Daily Practice

CLC/TS 50701 matters because it frames cybersecurity as an engineering lifecycle concern for rail systems and provides a practical structure operators can use to build repeatable assurance evidence.

Mature operators don't "implement CLC/TS 50701" as a document exercise, they use it to structure:

- Risk assessment and security requirements,
- Zone/conduit decisions and security levels,
- Change control and assurance evidence,
- Supplier acceptance criteria and lifecycle responsibilities.

8.3 Regulatory Readiness Based on Evidence, Not Declarations

Across regions, the enforcement trend is clear: regulators expect operators to quickly recognize significant incidents, coordinate responses, and report within tight timelines. NIS2's incident reporting obligations (including early warning and follow-on notification timeframes) are often characterized as explicitly time-bound, prompting operators to prioritize "always-ready" evidence collection and classification.

In the U.S., TSA's proposed "Enhancing Surface Cyber Risk Management" rulemaking similarly signals a shift from temporary directives to a more durable compliance regime for surface transport entities.

On the supplier/product side in the EU, the Cyber Resilience Act's scope and phased obligations reinforce that secure-by-design, vulnerability management, and lifecycle security are becoming procurement realities, not optional "security add-ons."

What credible readiness looks like (operator artifacts):

- incident classification tied to service impact and operational criticality,
- audit-ready evidence trails (asset state, changes, detections, supplier actions), exercised playbooks that involve operations/engineering, not just IT.

8.4 Detection and Response Integrated With Operations

In mature rail programs, detection is designed to answer an operational question: is this a real abnormality in rail behavior, a maintenance-driven change, a misconfiguration, or an intrusion? That requires monitoring and triage to interpret rail-relevant functions and constraints, and response processes built with operations/safety stakeholders so that containment decisions don't create unintended service or safety consequences.

8.5 The Integrated Operational Model of a Mature Operator

Pulled together, "good" in 2026 consistently means:

- continuous, rail-context visibility and segmentation discipline (zones/conduits),
- standards-driven engineering workflows (CLC/TS 50701 / IEC 62443 concepts),
- evidence-based regulatory readiness (not "paper compliance"),
- cyber + operations + engineering running one operating model.

And this is the key implication: many generic tools can contribute controls, but they don't automatically produce a rail-operational picture. The hard part, what leading operators invest in, is the unified, continuously maintained understanding of rail system boundaries, interdependencies, and expected behavior that makes assurance and response defensible.

Final Words

Rail's direction of travel is becoming consistent globally: more connectivity and interdependence mean more opportunities for disruption to cascade unless environments are deliberately structured and managed to contain it. The strongest rail programs aren't defined by "perfect prevention"; they're defined by maintaining an authoritative view of the environment, limiting how far disruption can spread, and restoring service predictably when something breaks.

The takeaway going into 2026 is simple: rail cyber maturity is measured by operational control, knowing what's connected, containing blast radius, and recovering fast with practiced, repeatable capability. The operators pulling ahead aren't chasing lawless prevention; they're building the muscle to keep operations steady through disruption.

About Cylus

Cylus provides advanced rail cybersecurity solutions, offering the first dedicated system to protect the entire rail OT and ecosystem. Cylus provides unparalleled visibility and threat detection across infrastructure, rolling stock, control centers, and stations, bringing all components into a unified security solution.

Trusted by rail operators and partners worldwide, Cylus helps ensure compliance with regulatory requirements and industry standards while maintaining safety and uninterrupted operations.
Backed by years of rail-specific innovation and global adoption, Cylus empowers organizations to protect their critical systems, detect threats early, and respond effectively, with confidence grounded in proven performance.

Appendix

Appendix A - Methodology

This paper is a structured synthesis of publicly available information and recurring operational patterns observed across the rail ecosystem. It draws on:

- Standards and engineering guidance relevant to rail OT cybersecurity (e.g., CLC/TS 50701, IEC/EN 62443, EN 50126 lifecycle alignment, emerging IEC 63452 workstreams).
- Regulatory and policy materials impacting rail and its supply chain (e.g., NIS2, Cyber Resilience Act, TSA surface cybersecurity rulemaking trajectory, national critical infrastructure regimes).
- Sector guidance and threat landscape reporting (e.g., ENISA transport/rail guidance, operator and industry association publications, national cybersecurity agency guidance).
- Publicly reported incidents and official updates from operators, authorities, and reputable media coverage, treated as examples of observable impact modes rather than a complete incident census.
- Public vulnerability disclosures and advisories (e.g., national CERT/CSIRT advisories, vendor PSIRTs, ICS advisory streams), used to identify repeatable exposure patterns relevant to rail OT and its component supply chain.

Analytic Approach

- Evidence-first framing: prioritizes what operators can demonstrate (repeatability, auditability, exercised response/recovery) over declared intent.
- Operational lens: interprets cyber impact primarily through service continuity, operational visibility, coordination capacity, and recovery friction.
- Cross-region comparison: highlights where practices converge globally while acknowledging differences in regulatory structure, procurement, and legacy architectures.

Appendix B - Limitations

- Public incident data is incomplete. Many rail incidents are never disclosed; those that are disclosed vary widely in detail. Trends in this paper should be read as publicly visible incidents, not total incident volume.
- Attribution is often uncertain. Public reporting may not reliably identify actor type, entry vector, or the true scope of impact; this paper avoids overclaiming when evidence is thin.
- Maturity statements are directional. They reflect observed patterns and sector guidance, not a statistically representative benchmark across all operators.
- Regional generalizations have exceptions. Legal obligations, enforcement maturity, and operator architectures vary significantly by country and by operator, even within the same region.
- Forward-looking timelines are subject to change. Dates tied to standards publication, regulatory enforcement, and guidance releases can shift based on voting, adoption, and implementation realities.

Appendix C — Acronyms

- AI — Artificial Intelligence
- APTA — American Public Transportation Association
- CRA — Cyber Resilience Act (EU)
- CSIRT / CERT — Computer Security Incident Response Team / Computer Emergency Response Team
- CISA — Cybersecurity and Infrastructure Security Agency (U.S.)
- CLC/TS — CENELEC Technical Specification
- DDoS — Distributed Denial of Service
- ERA — European Union Agency for Railways
- ERJU / EU-Rail — Europe's Rail Joint Undertaking
- ERTMS — European Rail Traffic Management System
- FDIS — Final Draft International Standard (IEC stage)
- FTA — Federal Transit Administration (U.S.)
- IACS — Industrial Automation and Control Systems
- IEC — International Electrotechnical Commission
- IPsec — Internet Protocol Security

- ISA — International Society of Automation
- IT / OT — Information Technology / Operational Technology
- KEV — Known Exploited Vulnerabilities (catalog)
- NIS2 — Network and Information Security Directive 2 (EU)
- NIST — National Institute of Standards and Technology (U.S.)
- NPRM — Notice of Proposed Rulemaking
- OEM — Original Equipment Manufacturer
- PSIRT — Product Security Incident Response Team
- RAMS — Reliability, Availability, Maintainability, Safety
- RED — Radio Equipment Directive (EU)
- RaaS — Ransomware-as-a-Service
- SBOM — Software Bill of Materials
- SCADA — Supervisory Control and Data Acquisition
- TSA — Transportation Security Administration (U.S.)
- UITP — International Association of Public Transport (Union Internationale des Transports Publics)
- UNIFE — Union des Industries Ferroviaires Européennes