Railroads & Cybersecurity

Through cybersecurity and incident response plans, railroads and industry organizations apply, assess, and continuously improve preparations, capabilities, and measures to protect information technology networks and operational technology systems. These sustained — and innovative — efforts reflect a unified commitment to ensuring the nation's critical rail infrastructure remains resilient against sophisticated cyber threats through mitigation and effective response.

Key Takeaway

The rail industry works cooperatively with government agencies, cross-sector and IT partners, law enforcement and security experts to protect the rail network from cyberattacks through sustained awareness, vigilant preparedness and effective responses.

A highly trained workforce helps protect the rail network.

Railroads and industry organizations recruit and retain highly skilled cybersecurity professionals who receive continual training to keep them abreast of current threats and best responses. Professional development is fostered through programs that elevate skills and capabilities for network defense through live exercises focused on detection, identification and disruption of varied types of cyberattack activity. Experience with actual incidents informs these scenarios.

Railroads address cybersecurity threats head on.

The Rail Information Security Committee (RISC) — an industry-formed and led coordinating group — is the focal point of the industry's unified, cooperative efforts for cybersecurity. The RISC is comprised of chief information security officers and information assurance officials for railroads and industry organizations, augmented by AAR security staff. Representatives of the seven Class I railroads and Amtrak established RISC in 1999, meaning the railroad industry has proactively enhanced cybersecurity through a dedicated forum for more than 20 years.

Intelligence sharing is crucial to cybersecurity efforts.

To bolster its cyber threat intelligence, the freight rail industry analyzes successful cyber intrusions and blocked attempts that have targeted private sector and governmental entities. In particular, the industry looks at the tactics most commonly used to gain illicit access to computer systems; vulnerabilities most commonly exploited; indicators of illicit activities most often noted in post-incident reports that were missed or disregarded and protective measures that could have made a difference.

- **Government Expertise**: The industry draws upon the experience and knowledge of experts at the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), Transportation Security Administration (TSA) Department of Defense (DoD), Department of Transportation (DOT), Transport Canada, and elsewhere to analyze cyberattacks and assist affected organizations.

- **Information Dissemination**: The industry-established Railway Alert Network (RAN) prepares and disseminates cyber threat alerts and advisories, with recommended protective actions, drawn from diverse sources.

- **Classified Threat Intelligence**: For classified threat intelligence, railroads and industry organizations maintain security clearances for cybersecurity leads; secure telephone and video-conference equipment for discussions of cyber threats and incidents at up to Secret level; and periodic contact with FBI and TSA intelligence officials in the areas of their headquarters and regional offices. RISC members — both those with security clearance issued by U.S. government organizations and by the government of Canada — participate regularly in classified in-person and remote presentations and briefings on cyber threats and incidents with analysts from the FBI, DHS, TSA and the National Security Agency (NSA).

Railroads and their security partners are committed to preparedness and continuous improvement.

- **Planning & Preparedness**: The railroad industry implements, continuously tests and improves a unified security plan as well as preventative and incident response plans. The unified security plan leverages defined and trained actions based on cyber and physical threat intelligence to mitigate risk as the level of a threat escalates. The response plans help railroads effectively respond to a cyberattack and safeguard business and operational technology networks and systems. Railroads regularly exercise and enhance these plans — both internally and as an industry — as well as train and test employees who use computer networks and devices to ensure they know how to appropriately address potential threats and concerns. An annual industry-wide exercise uses realistic scenarios and test plans to help ensure effective responses to cyber threats and incidents.

- **Assessments**: Individually and through the RISC, railroads conduct comprehensive cyber risk assessments based on realistic threat scenarios drawn from intelligence analyses, including "penetration testing" to evaluate networks and systems for vulnerabilities and needed enhancements. The RISC also evaluates industry cyber security plans and practices against international standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

- **Risk Mitigation**: A coordinated effort of the RISC has produced a compilation of effective practices to guide procurements — across the industry, by freight and passenger railroads of all sizes — of information technology systems, networks, software and supporting components. RISC members have engaged with suppliers to expand capabilities to assure mutual cyber threat awareness and facilitate design and development for mitigation of cyber risk in new systems.