Freight Rail: Protecting Physical & Cyber Networks

Key Takeaway: *Freight railroads use a layered, proactive strategy—coordinating with government, staying vigilant, and continuously improving—to keep their vast physical and digital networks secure and resilient.*

Freight railroads operate one of the world's most advanced and interconnected transportation networks, integrating extensive physical infrastructure with a sophisticated digital system for dispatching, logistics, and performance. To maintain safe and resilient operations, railroads safeguard both their physical and digital assets by investing in surveillance, intrusion detection, and fortified infrastructure, as well as enhancing cybersecurity through threat monitoring, defense frameworks, and public-private partnerships.

Cybersecurity

Freight railroads began coordinating their cybersecurity efforts in 1999, long before many sectors acknowledged the threat. In the aftermath of 9/11, the industry conducted a comprehensive risk assessment across operations, infrastructure, hazardous material shipments, military cargo, and communication systems. This proactive initiative established the foundation for a cybersecurity strategy that continues to evolve and adapt to emerging threats.

The Rail Information Security Committee (RISC)

RISC is the industry's central forum for cybersecurity leadership. Formed in 1999, RISC consists of chief information security officers and cyber leads from the major freight railroads, as well as Amtrak, and is supported by AAR security staff. RISC coordinates efforts and shares information on threats, effective protective measures, and risk mitigating actions. The Committee consistently communicates and collaborates with federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA), TSA, and the FBI. Working with these agencies, RISC shares threat intelligence, coordinates defense strategies, and responds to emerging cyber risks.

Cybersecurity Framework & Strategy

Freight railroads follow a cybersecurity strategy built on the guidelines and best practices developed by the National Institute of Standards and Technology (NIST). This flexible, proven framework helps railroads:

- Identify and assess cyber risks;
- Protect digital assets and operational systems; and
- Detect, respond to, and recover from cyber incidents.

Railroads regularly work with third-party cybersecurity experts to benchmark their programs against the NIST framework, including a biannual, industry wide benchmarking exercise. Internal audits and simulations further strengthen preparedness.

Dedicated Cybersecurity Teams

Each major freight railroad maintains a dedicated cybersecurity team, led by senior leadership in information security, including CISOs and their senior team leads. These teams oversee vulnerability management, threat detection and response, cyber risk assessment, and secure system architecture. They also run tabletop exercises and penetration tests to prepare for potential incidents and refine response plans.

Cyber Awareness & Training

Cybersecurity is embedded in the culture of freight rail. Employees receive regular training on secure data handling, recognizing phishing attempts, and reporting potential cyber threats. Railroads run cybersecurity awareness campaigns year-round, including simulated phishing tests incorporating the latest tactics used by malicious cyber actors. Cybersecurity liaisons within business units ensure cyber resilience is integrated into daily practices.

Physical Security

In the wake of the 9/11 terrorist attacks, freight railroads cooperatively developed the Rail Security Management Plan, a comprehensive blueprint of security enhancements and risk mitigation strategies. Implemented in 2002, the industry regularly updates the plan in partnership with federal agencies and intelligence experts to stay ahead of evolving threats. More than 130 North American railroads, including all major freight carriers operating in high-threat urban areas, have integrated the plan into their operations. A unified, intelligence-driven alert system outlines several threat levels that trigger escalating protective measures across both physical and cyber domains.

Safeguarding Against Cargo Theft

Since the COVID pandemic, freight carriers across all sectors have seen an increase in targeted cargo theft. Railroads have responded to these sophisticated criminal operations by bolstering their security efforts across the national rail network.

Railroads take extensive physical measures, dedicating millions of dollars towards deterrence of rail cargo theft. These comprehensive security efforts include actions like installing cut-resistant fencing, enhancing police/security guard patrols, and leveraging innovative technologies such as unmanned aircraft systems (UAS) and license plate identification technology.

Rail police and security personnel also implement operational best practices every day to actively deter and respond to crime targeting railroad operations. However, solving the cargo theft issue in the United States is much more complex than simply enacting best practices in rail environments. Ultimately ending these organized criminal operations demands law enforcement action and prosecution, something the railroads cannot do alone.

Security Exercises & Emergency Preparedness

Each year, freight railroads participate in the North American Railroad Industry Joint Security Exercise, a collaborative drill designed to test the Rail Security Management Plan, evaluate preparedness, and implement lessons learned. Participants include security and operations personnel from U.S. and Canadian freight and passenger railroads; industry IT leaders; and officials from the Transportation Security Administration (TSA), Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). Individual railroads also run internal initiatives to raise employee awareness and train emergency responders in the communities they serve.

Working Committees & Information Sharing

The Rail Security Working Committee (RSWC) brings together senior executives, police chiefs, and security staff from freight railroads, Amtrak, short lines, and commuter carriers. This group manages annual security reviews, conducts exercises, and collaborates with key government partners.

Employee Vigilance

Security starts with informed, alert personnel. Most rail employees receive security training during onboarding, followed by regular refresher sessions. This training focuses on identifying and reporting suspicious activity. Thanks to their vigilance, employees are responsible for the majority of threat reports in and around rail facilities—providing critical intelligence that supports coordinated responses with the TSA, FBI, Transport Canada, and other partners.