Freight Rail Security

Key Takeaway: Freight railroads work with government agencies and public partners to monitor every aspect of their physical and digital networks 24/7. Following a regularly updated comprehensive Security Management Plan, railroads share information and identify, mitigate and respond to risks. Since 1999, freight railroads have maintained a unified cybersecurity plan. The rail industry was one of the first to immediately review, test and update safety procedures based on new threats after 9/11.

In the immediate aftermath of the 9/11 terrorist attacks, railroads worked cooperatively to develop the rail industry's Security Management Plan. Put into effect in early 2002, the plan constitutes a comprehensive blueprint of security enhancement and risk-mitigating actions. Railroads regularly review, evaluate and update the plan in consultation with government and private security and intelligence experts to ensure continued effectiveness in the face of evolving security threats.

The unified, intelligence-driven approach maintains four alert levels that call for increasing physical and cybersecurity measures based on intelligence assessments and analyses of developing threats. More than 130 North American railroads — including all freight railroads that transport security-sensitive materials through high-threat urban areas — have integrated the security plan into their respective networks and operations.

Safeguarding Against Thefts

Since the COVID pandemic, railroads and other freight carriers 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. These comprehensive security efforts include actions like installing cut-resistant fencing, enhancing police/security guard patrols, and leveraging innovative technologies such as UAS and license plate identification technology.

Ultimately ending these organized criminal operations demands law enforcement action and prosecution, something the railroads cannot do alone. In many parts of the country, local law enforcement and local prosecutors have refused to take up these cases further incentivizing criminal activity.

Cybersecurity

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

Immediately following the 9/11 attacks in 2001, railroads came together to assess security risks. The assessments focused on operations, infrastructure, hazardous materials (hazmat) transportation, military shipments, and communications and computer systems with the goal of detecting and preventing terrorism.

Security Plan Testing

Each year, the rail industry and other critical infrastructure sectors participate in the North American Railroad Industry Joint Security Exercise to test the security plan, evaluate preparedness, and enhance capabilities and procedures using lessons learned. This exercise involves security, police and operations professionals from freight and passenger railroads in the U.S. and Canada; the security team and other functional staff from the AAR; IT leads from Railinc; and officials from government security and law enforcement agencies, including the TSA, DHS and FBI.

In addition to the industry-level exercise, each year, railroads engage in scores of individual company initiatives to evaluate and enhance employee awareness efforts and support emergency responders in the jurisdictions in which they operate. This collective effort reflects the sustained commitment across the industry to prevent and respond to physical and cyber threats.

Information Sharing

Timely and consistent information sharing increases security. The daily efforts of the Railway Alert Network (RAN) are a good example of the rail industry's commitment to information sharing. Since the implementation of the security plan in early 2002, the rail industry has maintained the RAN, managed by AAR, to serve as the security information center for North American railroads.

By analyzing evolving intelligence, the RAN supports security awareness through timely advisories and information briefs on potential terrorist tactics, malicious cyber activity, rail-related threats and incidents, and other suspicious activity. Railroads regularly use these materials in their employee security training and awareness programs. The RAN also shares security awareness information with counterparts in other transportation modes and government security officials in the U.S. and Canada.

Working Committees

Two industry committees work in collaboration with government agencies. The **Rail Security Working Committee (RSWC**) focuses on physical security and emergency preparedness, with senior executives, security staff, and police chiefs from major freight railroads, Amtrak, short line freight railroads, and commuter carriers. The RSWC conducts regular reviews of the industry security plan, manages the annual exercise program, and engages in open dialogue with TSA, DHS, the FBI, DOT, and Transport Canada to address security threats and enhance preparedness.

Established in 1999, the **Rail Information Security Committee (RISC)** coordinates unified cybersecurity efforts, comprising chief information security officers and information assurance officials. Supported by AAR security staff, RISC collaborates with federal cybersecurity agencies, including CISA, the FBI, and TSA, to share timely information on cyber threats and develop effective countermeasures.

Employee Vigilance

Rail employees play a vital role in protecting the network. Most U.S. freight and passenger rail employees receive security training during orientation upon initial hiring and continue with periodic sessions throughout their tenure. Training focuses on enhancing awareness and understanding indicators of potential security concerns and reinforcing timely reporting of observations per the procedures maintained by their respective railroads. The effectiveness of this regular security training is clear. Rail workers account for most reports of suspicious activity in and around rail facilities, facilitating effective industry coordination with and regulatory reporting to TSA, the FBI, Transport Canada and others. Their informed vigilance is essential.