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 programs strengthen network defense skills and capabilities through live exercises focused on detecting, identifying and disrupting cyberattacks.

**Protecting the Digital Network for More Than 20 Years**

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.

**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 Sharing**

Intelligence sharing is crucial to cybersecurity efforts. The freight rail industry analyzes successful cyber intrusions and blocked attempts targeting the private sector and governmental entities. Examples include reviewing the tactics used to gain illicit computer access, exploited vulnerabilities, illicit activity indicators in post-incident reports that were missed or disregarded and protective measures that could have made a difference.
The industry-established Railway Alert Network (RAN) prepares and disseminates cyber threat alerts and advisories, with recommended protective actions drawn from diverse sources. For classified threat intelligence, railroads and rail 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 maintain contact with FBI and TSA intelligence officials at their headquarters and regional offices.

RISC members — those with security clearance issued by U.S. government organizations and by the government of Canada — regularly participate in classified in-person and remote presentations and briefings on cyber threats and incidents with analysts from the FBI, DHS, TSA and NSA.

**Planning & Preparedness**

The railroad industry implements, continuously tests and improves a unified security plan and 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 threat level escalates.

The response plans help railroads respond effectively to cyberattacks and safeguard networks and systems. Railroads regularly exercise and enhance these plans — internally and as an industry — and train and test employees who use computer networks and devices to ensure they can 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**

The RISC has produced a compilation of effective practices to guide procurements by railroads of information technology systems, networks, software and supporting components. RISC members have engaged with suppliers to expand capabilities, assure mutual cyber threat awareness, and facilitate design and development for cyber risk mitigation in new systems.