Railroads and Cybersecurity

Association of American Railroads March 2018

Summary

To help ensure the security of their information technology networks and systems, **America's major railroads have taken proactive and multi-faceted steps to prevent, respond to, and build resiliency against cyber threats**. Implementing security programs guided by internationally recognized standards, **railroads perform thorough assessments of potential vulnerabilities; implement protective countermeasures; and recruit and train specialized cybersecurity staff**. Even the most effective cybersecurity plans and procedures will falter if useful information on cyber threats is not shared, which is why timely and comprehensive intelligence and information sharing between government security agencies and railroads is essential if cybersecurity efforts are to succeed.

Railroads Are Addressing the Cybersecurity Threat Head On

Railroads use computers and information technology in every aspect of their operations — train dispatching and tracking, detecting defects on cars and locomotives, operating switches in remote locations, scheduling maintenance, and much more. That's why cyberattacks are one of the main threats railroads work hard to protect against.

The **Rail Information Security Committee** (RISC) is the focal point of the industry's unified, coordinated cybersecurity efforts. The RISC is comprised of railroads' chief information security officers and information assurance officials, augmented by AAR staff and representatives of other industry groups. The RISC was formed in 1999 — meaning the rail industry had already established a forum for consultations and coordination on enhancing cybersecurity well before much more recent emphasis on it by government and businesses.

Working with public sector partners to share information on cyber threats and develop effective countermeasures is a key element of railroads' cybersecurity efforts. The industry's cyber threat intelligence priorities emphasize tactical analysis of successful cyber intrusions and blocked attempts that have targeted private sector and governmental entities. This focus draws upon the experience and knowledge of experts at the Department of Homeland Security, the Federal Bureau of Investigation, Transport Canada, and elsewhere in analyzing cyberattacks and assisting affected organizations.

In particular, the rail industry seeks analyses that highlight tactics that are most commonly employed to gain illicit access to computer systems; vulnerabilities most commonly exploited; indicators of illicit activities most often noted in post-incident analyses that were missed or disregarded; and protective measures that could have made a difference.

Railroads enhance their cybersecurity in a number of other ways, including:

- Maintaining **cybersecurity incident response plans** that are tested regularly and enable preparedness to act effectively in case of a cyber-attack.
- Incorporating a variety of safeguards into their business and operational practices, such as tools to **enhance capabilities for continued operations under adverse conditions** and protocols that **only allow authorized personnel access to key IT systems**.
- Conducting regular comprehensive **vulnerability assessments** (including "penetration testing" that simulates an attack from malicious outsiders) and participating in recurring, coordinated industry- and government-sponsored **cybersecurity exercises**.
- **Hiring highly skilled cybersecurity professionals** who receive continual training to keep them abreast of current threats and best responses.
- Increasing the use of **software and other technologies to detect and quarantine cybersecurity threats**.

What Cybersecurity Legislative Proposals Should Address

Railroads agree that increasing cybersecurity is vitally important. To this end, they urge policymakers to support cybersecurity legislation that adheres to the following guidelines:

- Even the most effective cybersecurity plans and procedures will falter if useful information on cyber threats is not shared, which is why **timely intelligence and information sharing is essential** if cybersecurity efforts are to succeed. The focus should be on sharing tactical intelligence on what perpetrators are doing and how they are doing it.
- **Overly prescriptive regulatory requirements should be avoided** because the measures they require are quickly outstripped by a constantly evolving, dynamic threat. Adherence to obsolete requirements stifles innovation. Instead, policymakers should rely on cooperative efforts through performance-based approaches that focus attention and effort on the outcome, not the method. A performance-based approach assures the flexibility and adaptability required to confront ever-changing cyber threats.
- Attention should be focused on the primary cause of cybersecurity vulnerabilities — inadequate attention to security in the development and production of IT hardware and software — rather than on requirements or standards for end users.
- Great care must be taken to ensure that **commercially sensitive information** on cyber incidents and cyber threats reported to the government is **protected from inappropriate uses or public disclosure**. The damage to firms' reputations and potential liability from misuse or careless handling of this sensitive information can be substantial and enduring.
- **Existing federal entities with cybersecurity responsibilities should be streamlined** to help ensure that useful intelligence and security information is shared in a timely, effective, and consistent manner.
- **Mandated certification requirements or standards for cybersecurity workers are unnecessary in the rail industry** because railroads already use extensive background checks and other means to identify job applicants who might pose a security risk.