1898 & CO.
PART OF BURNS & McDONNELL

WHITE PAPER

Solving for Cybersecurity Threats in the Rail Industry: Risk Assessment and Segmented Technology

By Robert Bradford and Nathan Brown

Cybersecurity threats and ransomware attacks have increased in frequency, putting railroad companies in a vulnerable position. In response, the Transportation Security Administration issued a new directive for railroad companies to enhance cybersecurity resilience using performance-based measures. Railroad companies that prioritize network segmentation, monitoring, detection and access control measures can mitigate preventable risks.

Supply chain issues triggered by the COVID-19 crisis continue to encumber consumers, businesses and policy leaders. And while intermodal movement is progressing toward pre-pandemic levels, other factors outside of the pandemic are poised to continue endangering freight rail and the supply chains supported by this industry. Specifically, ransomware attacks and cybersecurity threats could disrupt supply chains, damage critical infrastructure and possibly cause loss of life.

In 2021, ransomware attacks compromised two other components of critical infrastructure: pipelines (Colonial Pipeline) and food processing (JBS Foods). While most railroads have long-established internal cybersecurity teams focused on enterprise information technology (IT) systems, significant technologies have been deployed to the field that have not always followed cybersecurity best practices. These field systems have been created in response to the positive train control (PTC) initiative, and due to the effort and regulatory time commitments, cybersecurity was not a primary concern during the deployment of PTC technologies. This creates vulnerabilities that need to be addressed by most freight railroad companies.

In October 2022, the Transportation Security Administration (TSA) instituted a new security directive for freight and passenger carriers. Under this directive, railroad companies must create network segmentation controls and policies, develop access control measures, establish monitoring and detection policies and procedures, and mitigate potential exploitation of unpatched systems. Network segmentation controls and policies should give railroad companies a framework to maintain operational technology (OT) when IT is jeopardized. Effective access control measures should mitigate unauthorized access, while monitoring and detection policies and procedures are intended to help railroad companies detect, respond and recover from cybersecurity threats and attacks. Prioritizing is critical as cyber attacks will be inevitable in the railroad sector. Finally, railroad companies can safeguard against the exploitation of unpatched systems by implementing security patches and upgrading applications, drivers, operating systems and firmware. Ransomware attacks are continuously evolving but generally are designed to encrypt files so that they are unusable by an organization until the malicious actor who instigated the attack is compensated. In 2019, there was a ransomware attack every 39 seconds. In 2021, ransomware attacks occurred every 11 seconds.

Within the railroad industry, ransomware attacks could be used to cripple the systems designed to plan train movements, forcing the railroad to return to paper-based planning mechanisms. With the implementation of the PTC rules — and assuming any ransomware attack would remove PTC functionalities — trains effectively could be running at restricted speeds. The addition of the PTC field systems also opens up a new threat vector that could be exploited to deliver a ransomware attack via systems that might not be effectively monitored.

In addition to the cybersecurity requirements issued by TSA in 2022, railroad companies can reduce cyber-risks using an established framework and implementation guide prepared by the Cybersecurity and Infrastructure Security Agency (CISA), an operational agency under the Department of Homeland Security (DHS). The work of TSA and DHS is critical to identify risks and vulnerabilities that vendors and cybersecurity professionals can address. Unfortunately, attacks are occurring more frequently, leaving railroad companies more vulnerable in the near term, unless they take action themselves. Railroad companies can take proactive steps today using the guidance from CISA and the Association of American Railroads (AAR) in tandem with any new federal regulations to improve their cybersecurity defenses.

Financial Implications for the Rail Industry

In a 2017 study conducted by Towson University, Class 1 railroad operations and capital investment supported $219.5 billion in economic output and $71.3 billion in wages annually. Additionally, these operations and capital investments supported more than 1.1 million jobs. With current limitations hampering supply chains, the ability to quickly move freight is more important now than ever. Additional disruptions within supply chains due to railroad issues would exacerbate an already delicate scenario.

If a hacker can target railway control centers via ransomware or a cybersecurity attack, the risks to the economy, as well as people and the natural environment, can be devastating. While disruptions to supply chains can lead to higher costs and shortages of products, railroads also transport hazardous materials that can be damaging to the environment and people. With the newly implemented control systems on locomotives and at control points, cybersecurity attacks have the potential to derail trains or override directives which could lead to collisions resulting in hazardous spills or crashes. These potential threats underscore the critical need to secure systems both within railroad datacenters and in the field to support train operations.

How Rail Systems Moved Toward Positive Train Control

In September 2008, a Union Pacific freight train and a Metrolink passenger train collided in California resulting in the deaths of 25 individuals. More than 135 passengers were injured. In October 2008, President Bush signed the Rail Safety Improvement Act (RSIA) of 2008, which required most rail networks to adopt PTC technology by December 2015.

PTC is a system designed to monitor and control train movement with the intent of protecting trains, freight and passengers. In simple terms, PTC systems deliver autonomous control of a train to offset human error. In North America, the model for PTC focuses on trains receiving location information and guidance for safe travel. These communications happen via a vast network of interconnected systems incorporating long-term evolution (LTE) technologies, Wi-Fi and data radios that are all supported via a messaging system that connects all interoperable railroads together.

While the RSIA called for the installation of PTC systems, the act doesn't require a specific technology. Instead, RSIA outlines goals for PTC systems, such as enforcement of speed limits, stopping trains from entering work zones and mitigating collisions between two trains.

There are obvious benefits to implementation of PTC technology. It's estimated that from 1987 to 1997, PTC-preventable accidents accounted for a yearly average of seven fatalities and 22 injuries. The mitigation of these accidents is a fantastic development for the rail industry, but the PTC technology is susceptible to cyberattacks. Furthermore, issues within the systems of one railroad can now progress across partner railroads, opening up additional threat vectors and creating additional vulnerabilities to the overall operations of the railroads.

Segmenting IT from OT

A common approach for reducing the likelihood of a cyberattack is segmenting IT from OT. Today there is a convergence of IT and OT systems taking place across various industries. IT refers to the use of computers, networks and storage systems to process, create, store, exchange and secure electronic data. OT, on the other hand, refers to the hardware and software that identifies or initiates changes by monitoring and controlling industrial equipment and processes.

Within the railroads, these OT systems exist at control points, on locomotives and extending into the back office due to the PTC messaging system. This opens up substantial vulnerabilities that need to be addressed and managed. While separating these systems via strong access controls and firewalls does create operational obstacles, it also enhances the safe operations of these systems and reduces the likelihood of a cyberattack affecting one railroad and then traversing the PTC network to additional railroads.

Most cybersecurity systems focus on building a perimeter around an organization's IT infrastructure to keep out hackers. While this is an important step, railroad companies should consider instituting multiple mechanisms to protect the network. Specifically, railroad companies could implement a defense-in-depth (DiD) strategy, which requires multiple security controls and mechanisms incorporated throughout a computer network. A railroad company's DiD strategy may include network segmentation, firewalls, intrusion prevention or detection systems, patch management and strong passwords. Implementing a DiD strategy can require more time, energy and resources to establish, but the upfront work has long-term benefits. Companies that pursue a DiD strategy are making their networks more complex, thus making it more difficult for hackers to attack networks and IT systems.

Developing a Risk Assessment

To protect the informational and operational technologies administered by railway entities, start with an adversarial mindset. An internal risk assessment is something rail entities can do today to improve their cyber posture. Consider th following steps:

- Catalog assets and identify the most critical assets.
- Identify, describe and assess distinct threats.
- Assess the vulnerabilities of your critical assets.
- Determine potential risks and the consequences of different types of attacks.
- Outline steps to reduce risks.
- Prioritize risk reduction efforts based on a thoughtful strategy.

More information about how to conduct a risk assessment is available on the CISA website.

Understanding the Cybersecurity Framework (CSF)

The National Institute of Standards and Technology has established a Cybersecurity Framework (CSF) that can be adopted by railroad companies to protect themselves and manage a cybersecurity attack. While many organizations focus on the protect and detect areas of cybersecurity, many times the response and recovery scenarios are not as well defined. Assessing and creating a plan for all categories is critical for the security of railroad companies.

***Figure 1:** The Cybersecurity Framework (CSF) was developed by the National Institute of Standards and Technology. It includes five different activities to help asset owners achieve specific cybersecurity outcomes.*

CISA, an agency of the U.S. Department of Homeland Security, recommends that companies develop an incident response plan (IRP) for cybersecurity attacks. An IRP is a written document that clearly defines how an organization should respond to a cyberattack. The IRP outlines roles and responsibilities, and will identify essential staff needed to mitigate damage.

Unified Efforts to Address Cybersecurity

Core business activities for railroad companies are mostly dependent on IT and how that technology is incorporated into business operations. Railroad companies are collaborating with industry partners to share current cybersecurity intelligence. The industry also benchmarks its security using universally recognized standards and successful procedures. AAR manages a committee to address cybersecurity threats. This committee assesses individual railroad's information assurance programs, shares information with government agencies and develops security benchmarking activities that align with cybersecurity guidelines. The committee also shares relevant information on the Railway Alert Network, which was developed by law enforcement agencies, rail labor groups, railroad companies and the Federal Railroad Administration (FRA) to distribute information and intelligence on security issues in a timely manner.

Conclusion

Testing IT and OT systems and business operations is necessary to evaluate a company's preparedness. After implementing appropriate protective strategies and segmenting OT from IT technology, railroad companies will need to conduct penetration testing and red teaming on PTC networks. A red team includes cybersecurity professionals hired to behave as hackers or malicious actors. The red team will try to circumvent cybersecurity systems while infiltrating the system. This type of test will help railroad companies identify vulnerabilities.

Using resources provided by CISA, FRA and AAR, railroad companies can develop plans to address safety, economic and environmental concerns. Specifically, an effective IRP is essential to minimize damage and support business operations. With an IRP in hand, railroad companies can run tabletop exercises to prepare for cyberattacks.

Railroad companies must contend with the reality that a cyberattack will happen. Railroad companies that test systems, enhance cyberdefenses and plan for the worst-case scenario will be well positioned to minimize or avoid potential cyberthreats or malware attacks, while enhancing the resiliency of a country's supply chain and transportation networks.

About 1898 & Co.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.

62102-0123