

IN NEED OF CYBER RESILIENCE

Rail has been slow to modernize, but it can't drag its feet on cybersecurity any longer

Patrick Lortie • Paul Mee • Brian Prentice

THE WORLD ECONOMIC Forum's most recent "Regional Risks of Doing Business" report lists cyberattacks as the top concern of corporate executives in 19 countries, including advanced economies in North America, Europe, and Asia. These concerns, according to the report, "highlight the growing reliance of global commerce on digital networks that are the target of increasingly sophisticated and prolific attacks." And not surprisingly, most highly digitized industries and companies—many of which have experienced cybercrime firsthand—are incorporating cybersecurity into their cultures.

That is, most but not all. The rail industry, with legacy infrastructure built long before the internet, appears to be dragging its feet, even as it increasingly relies on expanded digital systems and connectivity and the world moves toward autonomous operation of transportation.

Globally, trains offer relatively soft and highly tempting targets for those looking to wreak havoc, as rail is often closely tied to a country's economic infrastructure and mobility. In the United States and elsewhere, rail freight often includes dangerous industrial goods, while passenger rail is a common mode of travel in most countries, except the US, especially in and around densely populated urban cores.

What's more, the rail sector has witnessed its share of cyber events. In 2008, a 14-year-old boy modified a television remote to change junction-box controls and derailed four trams in Lodz, Poland, injuring passengers. The rail network in the United Kingdom was attacked four times in 2015 and 2016 by hackers exploring its vulnerabilities; Canada's Metrolinx thwarted a 2017 cyberattack originating in North Korea. Meanwhile, ransomware and distributed denial of service attacks have shut down systems ranging from scheduling and information to internal communications and ticket selling at the San Francisco Muni, Deutsche Bahn in Germany, and Danish train operator DSB. While not crippling, these forays hint at the potential for damage and indicate that it's high time for the industry to develop more cyber resiliency.

The scope of risk

There are as many as 300,000 hackers worldwide, and that number is growing. Organized crime, hacktivists, and nation states are part of the mix and constantly innovating, meaning that the severity and frequency of attacks is likely to increase.

Rail networks are particularly at risk because they are extensive, dispersed, and complex. Despite modernization, critical infrastructure is still made up of legacy components not originally designed and deployed with cyber resilience in mind. Transportation systems also are increasingly interconnected and connected to the internet. The continued introduction of new and connected technologies, such as Internet of Things sensors and tools, further widens the "surface area" vulnerable to cyberattack. The introduction of machine-learning and artificial intelligence is expected to lead to even more potent and targeted cyberattacks.

In the US, the rollout of positive train control (PTC) on 65 percent of the rail network could be of notable interest to bad actors. PTC represents a new application of a complex web of technologies, such as GPS, wireless, cellular, and radio communication, and PTC installations have largely eliminated legacy signal systems that were air-gapped. PTC is designed to improve rail safety by preventing train collisions and derailments, yet its cyber vulnerabilities and security weaknesses might be easily exploited, thus creating new safety concerns.

Other liabilities include the use of open-source software and software with outdated security patches (which the 2017 WannaCry ransomware attack exploited). In addition, railroads, like other asset-intensive industries, typically do not have a culture of cyber awareness, which makes their workforces vulnerable to social engineering, such as phishing, and the misuse of portable storage and other intrusion-enabling devices.

Finally, technology architectures typically contain legacy components from third- and fourth-party providers, making vulnerabilities, often deep in the technology stack, difficult to discern and address. Hardware as well as software is exploitable; for example, the Chinese government reportedly infiltrated the networks of major US corporations by inserting nearly undetectable microchips into computer servers built by Chinese companies. This has led to US lawmakers expressing concerns over state-owned China Railway Rolling Stock Corp. bidding on a contract to supply new rolling stock for the Washington Metro. In response, the Metro has tightened cybersecurity requirements for the tender, but some doubt these go far enough.

An attack's fallout

The cyber risks for rail are many, including financial losses, compromised infrastructure, scheduling and communications breakdowns, theft of private data, safety liabilities, and reputational risk. In the EU, scheduling and information blackouts have shut down trains and stranded passengers, leading to lost revenues and network disruptions. The most serious concern, of course, is the physical safety of the rail network. PTC, digitally controllable locomotives and train components, and expanding wireless data streams all make the threat of a hacker-caused train collision or derailment real.

Beyond direct financial losses, post-attack recovery can be costly: When JPMorgan Chase was hacked in 2017, direct losses in the millions were followed by cybersecurity investments—over \$500 million in the year that followed the incident. Similarly, the world's largest shipping company, A.P. Moller-Maersk, was hit by ransomware in 2017 that disrupted operations at terminals in four countries for weeks, generating recovery costs of up to \$300 million.







Concerns over the potential impacts of cyberattacks also raise the threat of additional regulation or shipper requirements that railroads guarantee the integrity of product and transportation data. Stricter cybersecurity laws may be in the offing for infrastructure considered critical to a country’s economy and security. The EU, for example, has implemented a Network and Infrastructure Security directive to standardize cybersecurity protocols for “essential services,” while the US created the Cybersecurity and Infrastructure Security Agency (CISA) as a new federal regulatory agency in late 2018.

Beefing up defenses

Cyber resilience—the ability to prepare for, react to, and move past a cyberattack—must be high on the agenda of rail executives and board members. Fortunately, railroads can learn from and in some cases leapfrog other industries that have experienced daunting cyberattacks firsthand, such as finance and healthcare.

Most critically, an organization’s outlook in terms of preparedness for cyberattacks needs to be a “when—not if” mentality. Railroads should assume a cyberattack will happen and develop a robust and responsive risk-management system. This starts

FEATURES OF AN ADEQUATE CYBER ASSESSMENT

	RISK MEASUREMENT	Fully understand cyber risk exposure and the underlying drivers of losses.
	RISK MANAGEMENT	Ensure that cyber risk can be comprehensively managed across the organization.
	RESPONSE	Be prepared to respond quickly and in a structured way to a cyberattack, to minimize stakeholder impact.
	INVESTMENT PORTFOLIO	Evaluate investments across the cyber risk mitigation spectrum and relative to other investment demands.
	EXECUTIVE OVERSIGHT	Continuously monitor cyber risk exposure status, trends/outlook, and the impact of investments.
	INSURANCE	Determine cyber coverage strategy and the nature/extent of premiums.

Source: Oliver Wyman analysis

with asking the right questions to fully understand the threat landscape and all the components of risk and response that must be developed and managed.

Effective cybersecurity begins by articulating a strategy in response to these questions, supported by an assessment of the company's current preparedness, appetite for risk, and quantification of economic exposure. A cyber operating model can be used to assign roles and responsibilities, while a cyber dashboard can monitor threat metrics and elevate discussion to the executive/board level. Finally, cyber playbooks need to be developed that step through how to handle major incidents, including accountabilities and response/recovery actions.

A valuable input to this process can be simulating various attacks on the organization, based on the threat landscape and prior attacks on other companies, to determine preparedness and resiliency. Working sessions with employees can uncover their knowledge about specific security weaknesses and gaps in oversight, controls, and access.

Railroads are complex, unique environments. Managing cyber risk and building appropriate defenses for railroads are not easy tasks, given the mix of legacy components that railroads have inherited and the advanced technologies they are embracing. But make no mistake: Cyber resiliency is a clear and urgent necessity in today's digital world.

Patrick Lortie

is Oliver Wyman's global rail practice leader and a partner based in Montreal.

Paul Mee

is a New York-based partner in Oliver Wyman's digital, technology and analysis practice.

Brian Prentice

is a Dallas-based partner in Oliver Wyman's transportation and services practice and its operations practice.

This article first appeared in [Railway Age](#) on March 21, 2019.