Gallagher

ON THE RIGHT TRACK

Managing Cyber Risks in the Railway Industry

In Brief

Rail operators are adopting new technologies to enhance efficiency and improve passenger experience. However, these innovations also expand the cyber attack surface. Secure-by-design principles and adaptive risk management are key to staying ahead.

Traditional property and casualty policies often exclude cyber-related events. Modern cyber insurance fills these gaps with tailored coverage and proactive services, including incident response.

Mapping vulnerabilities across IT (information technology) and OT (operational technology) systems and conducting risk quantification helps operators prioritize investments and align insurance coverage with actual risk.

The railway industry, once largely analog, is undergoing a sweeping digital transformation. Internet of Things (IoT) devices, automation, cloud platforms and AI-driven analytics are redefining rail operations by enabling predictive maintenance, streamlining processes like signaling and ticketing and providing real-time data access across systems.

These technologies improve efficiency, safety and passenger experience through optimized operations and personalized services. However, this interconnected ecosystem also introduces new threats and vulnerabilities, making cybersecurity and risk management a critical priority.

Cyberthreats are no longer hypothetical across the rail industry. Ransomware attacks, where hackers seize and encrypt valuable data, demanding payment to release it and sophisticated system breaches have disrupted rail operations worldwide, exposing weaknesses in both information technology (IT) and operational technology (OT) environments.

A successful cyber attack can do more than compromise data. It can halt train operations, disable safety systems and erode public trust. Such attacks can lead to financial losses, privacy litigation, regulatory proceedings, reputational impacts and even physical damage.

"The more educated and aware the rail industry is about existing and emerging risks, the better prepared it will be to respond to potential cyber attacks," says Kevin Woods, managing director of the Rail Transportation practice at Gallagher.

This whitepaper examines the evolving threat landscape and offers practical strategies for resilience. It offers a starting point for rail operators seeking to better understand risks and prioritize cybersecurity improvements and investments to move forward with confidence.

The more educated and aware the rail industry is about existing and emerging risks, the better prepared it will be to respond to potential cyber attacks.

— **Kevin Woods**
Managing Director of Rail Transportation practice
Gallagher

Understanding Cyberthreats to the Railway Industry

As rail operations today depend on a complex web of digital systems, hacking into the invisible infrastructure that enables them is a top concern for operators.

A breach in OT technology could compromise signaling systems, passenger information platforms, traffic management systems or in extreme cases, train control systems. While large-scale attacks on Positive Train Control (PTC) systems have not yet occurred, the possibility of such an event keeps rail operators on high alert.

On the IT side, common exposures include locked internal systems, blocked dispatch operations, and ransomware attacks targeting sensitive customer or employee data, including biometric data. However, rail operators need to remain knowledgeable about regulations like the Biometric Information Privacy Act (BIPA) that have led to an increase in privacy claims. At the same time, outdated infrastructure and human error amplify these risks, while growing interconnectivity broadens the attack surface.

Most pressing cybersecurity challenges for **commuter/passenger rail**

- Incident response
- Privacy liability and privacy regulation
- Cyber extortion
- Business interruption
- Dependent business interruption

Most pressing cybersecurity challenges for **freight and cargo rail**

- Incident response
- Cyber extortion
- Business interruption
- Impact on the operational technology environment (Centralized Traffic Control — CTC, Positive Train Control — PTC, Supervisory Control and Data Acquisition — SCADA systems)
- Physical damage events
- Business interruption arising from physical damage events

A sector in transition

The current migration in the US rail industry from Global System for Mobile Communications - Railway (GSM-R) to the Future Railway Mobile Communication System (FRMCS) marks significant progress. However, many systems still rely on outdated OT infrastructure and IT platforms that lack modern cybersecurity safeguards.

"This is not an overnight fix. Many organizations are lacking proper infrastructure and are significantly behind where they need to be in terms of cybersecurity, sometimes without knowing," explains Brad Burtram, executive director for Rail at Gallagher. "The problem is that bad actors are incredibly advanced and almost always a step or two ahead, which means we're constantly trying to play catch-up."

> Many organizations are lacking proper infrastructure and are significantly behind where they need to be in terms of cybersecurity, sometimes without knowing. The problem is that bad actors are incredibly advanced and almost always a step or two ahead, which means we're constantly trying to play catch-up.

— Brad Burtram
Executive Director for Rail
Gallagher

The IT-OT convergence challenge

The growing use of technology has increased connectivity between IT and OT systems, creating a tighter interface. This integration improves efficiency and enables real-time decision-making in rail operations, but it also heightens risk.

Because these systems are increasingly interconnected, such as through IoT sensors, a breach in one can quickly cascade across the entire network. Moreover, the traditional view of cyber risk, mainly focused on data privacy and "air gapping" OT systems so that hackers could not gain access, is no longer sufficient.

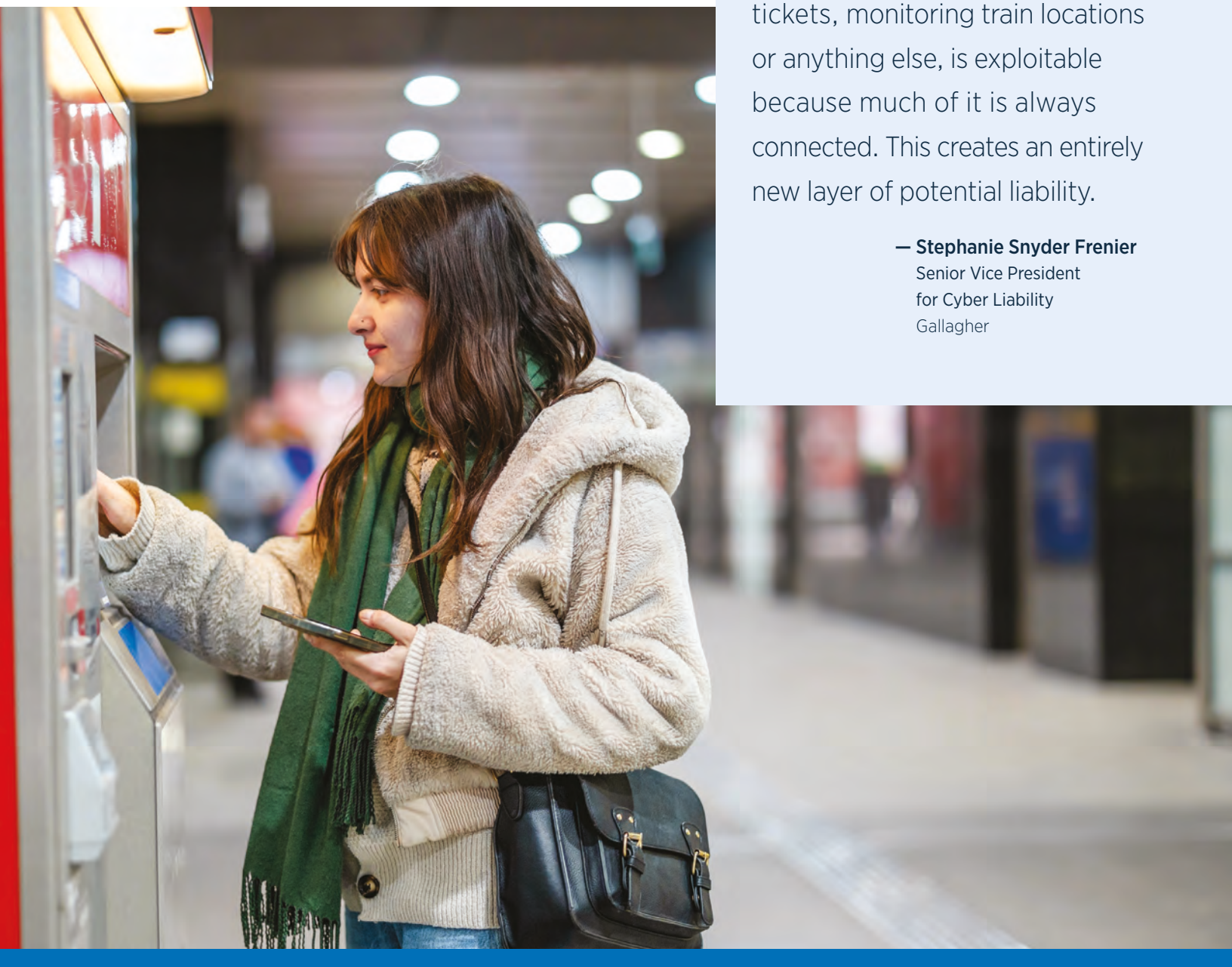
"Any type of technology being used, whether it's for buying tickets, monitoring train locations or anything else, is exploitable because much of it is always connected," explains Stephanie Snyder Frenier, senior vice president for Cyber Liability at Gallagher. "This creates an entirely new layer of potential liability."

Emerging threat vectors

Risks also arise from less obvious sources. Website tracking technologies, for example, can expose rail operators to litigation as these tools collect data subject to privacy and compliance requirements.

"We are seeing now more cases where websites have embedded videos, pixel tracking technologies or chat functionalities which can lead to significant litigation and potentially trigger cyber policies," explains Snyder Frenier.

> Any type of technology being used, whether it's for buying tickets, monitoring train locations or anything else, is exploitable because much of it is always connected. This creates an entirely new layer of potential liability.
>
> — **Stephanie Snyder Frenier**
> Senior Vice President
> for Cyber Liability
> Gallagher



Supply chain and geopolitical vulnerabilities

The digital supply chain offers both opportunities and vulnerabilities for all operators seeking to improve their cybersecurity. The rail industry's growing reliance on third- and fourth-party vendors for security and operational software introduces additional layers of exposure.

"Organizations need to gain visibility into their technology suppliers and establish communication protocols for cyber incidents," advises Nick Gwynne-Robinson, consultant for Crisis and Security Strategy at Another Day, a Gallagher company.

Large rail operators are increasingly requiring suppliers to carry cyber insurance as a prerequisite for doing business, recognizing the shared responsibility in securing the ecosystem.

Global geopolitical events can also influence cyber risk, and rail, as part of the infrastructure that moves the global economy, is often targeted in this unstable backdrop. In 2025, 60% of global organizations identified geopolitical tensions as a driver for changes in their cybersecurity strategy, and 45% of cyber leaders point at operations and business disruption as their top concern.[2]

Timeline of Cyber Attacks on Rail Operators

US 2023
Ransomware attack and exfiltration of approximately 80 GB of data.

Poland 2023
Emergency stoppage of around 20 trains due to compromised railway radio frequencies, triggering the train emergency stop function.

New Zealand 2023
A ransomware attack disrupted ticketing and customer service systems. Subsequent Denial of Distributed Service (DDoS) attack allegedly for not paying ransom.

UK 2024
Cyber attack exposed customer information, required employee password resets and disrupted operations — including live arrival information and payment processing.

UK 2024
Hacking of Wi-Fi at railway stations caused terror messages to be displayed on devices.

France 2024
A ransomware attack disrupted ticketing and scheduling systems for a major commuter rail operator.

US 2024
A ransomware attack left operators unable to see where railcars were located for almost four hours.

What Can Cyber Insurance Do for Rail Operators?

Despite the rail industry's awareness of the need for appropriate cybersecurity controls as it adopts new technology, underinsurance remains a critical issue.

Budget constraints, exacerbated by reduced commuter traffic and revenue declines since the pandemic, have further limited investment in cybersecurity and insurance. "Rail organizations are embracing enhanced internal cybersecurity controls to address these technological changes, but many do not have adequate coverage to protect against loss," explains Snyder Frenier.

Beyond coverage: added value

Traditional property and casualty (P&C) insurance policies often fail to address cyber-specific risks, leaving rail operators exposed to financial, operational and reputational harm. Cyber insurance addresses these gaps by providing specialized coverage for digital threats, including:

- Breach response costs (legal, public relations and crisis management)
- Security and privacy liability
- Data breach notifications and privacy regulatory proceedings
- Business interruption and dependent business interruption
- Cyber extortion and ransom
- Reputational harm
- Computer hardware replacement

"Carriers aim to help organizations prevent claims in the first place. They provide access to and indemnification for a variety of value-added services beyond just the financial protection," says Snyder Frenier. Such expert resources and proactive risk management services can include:

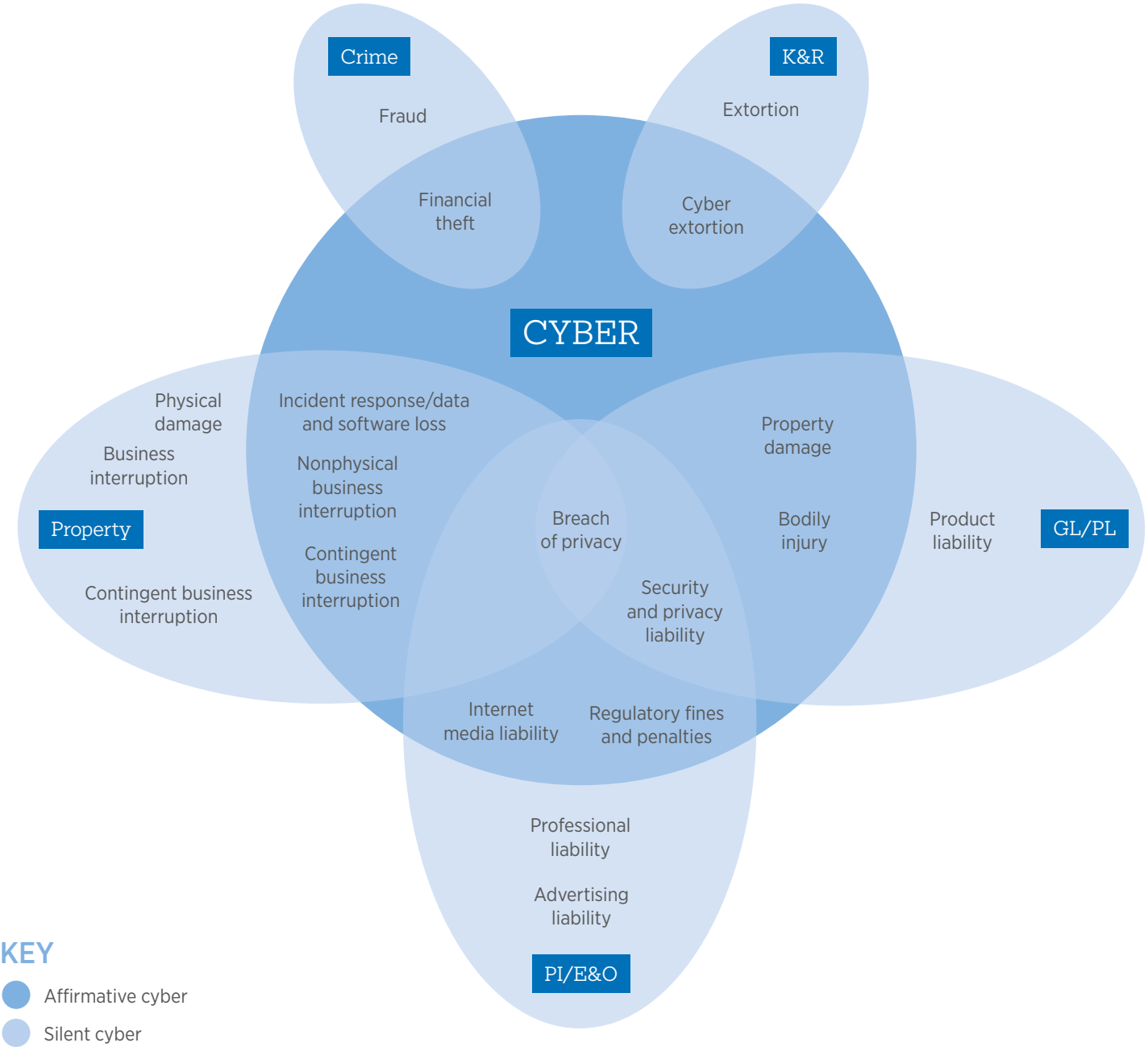
- Incident response support and legal counsel
- Data forensics and credit monitoring
- Complimentary or discounted services like tabletop exercises, dark web monitoring, penetration testing and vulnerability scans

"Insurance carriers providing cyber coverage understand the complexity of this industry. For operators with small IT teams, these external support services can be essential," describes Woods.

In a cyber incident, timing is crucial. Specialist advisors can evaluate the situation, guide recovery efforts and offer additional support in legal, public relations and crisis management to reduce damage and speed up recovery.

Falling Short with Traditional Cyber Insurance

Traditional insurance policies have significant gaps in coverage for cyber exposures and often have broad coverage exclusions that leave your company vulnerable. Custom programs are critical to protecting your business against the traditional and nontraditional impacts a cyber crisis can have on your business.



KEY

- Affirmative cyber
- Silent cyber

PI/E&O: Professional Indemnity/Errors & Omissions
GL/PL: General Liability/Product Liability
K&R: Kidnap and Ransom

Source: The Cyber Frontier, Gallagher

Potential Cyber Limitations in Traditional P&C Policies

Property & Casualty (P&C) insurance policies have historically been a key part of risk management for rail operators, covering physical damage and third-party liability. However, these policies often fall short of addressing the changing landscape of cyberthreats.

Why addressing silent cyber left gaps in traditional policies

Before 2019, most P&C insurance policies covered damage caused by cyber-related events, such as when a cyber attack resulted in a fire, explosion or machinery breakdown.

Starting in 2020, in an effort to address the issue of "silent cyber" — a term used to describe potential cyber exposures that are neither explicitly included nor excluded in traditional insurance policies — the Lloyd's of London insurance market required insurers to clearly state whether cyber risks were covered or excluded. As a result, insurance carriers have added cyber exclusions to their P&C policies, leaving some businesses without coverage for damages stemming from cyber incidents, whether malicious (like hacking) or non-malicious (like system errors), even when they cause tangible physical damage.

Why rail operators are exposed to cyber-physical and non-damage business interruption

As a sector heavily reliant on OT systems, cyberthreats in the rail industry may cause direct physical harm, including equipment destruction, system failures and safety hazards, which could in turn lead to bodily injury.

To address these exclusions, the market introduced "buyback" solutions that allow operators to purchase additional coverage. For example,

- **Affirmative Basis:** Fully buying back cyber exclusions, whether related to malicious or non-malicious events, such as property damage or bodily injury.
- **Non-Affirmative Basis:** Selectively buying back specific exclusions under the policy, tailored to what the insured is most concerned about.

"These buyback options allow rail operators to address specific exclusions and close critical gaps in their P&C coverage," says Joe Stubbings, director for Large Corporate Cyber practice at Gallagher.

The role of education and advisory

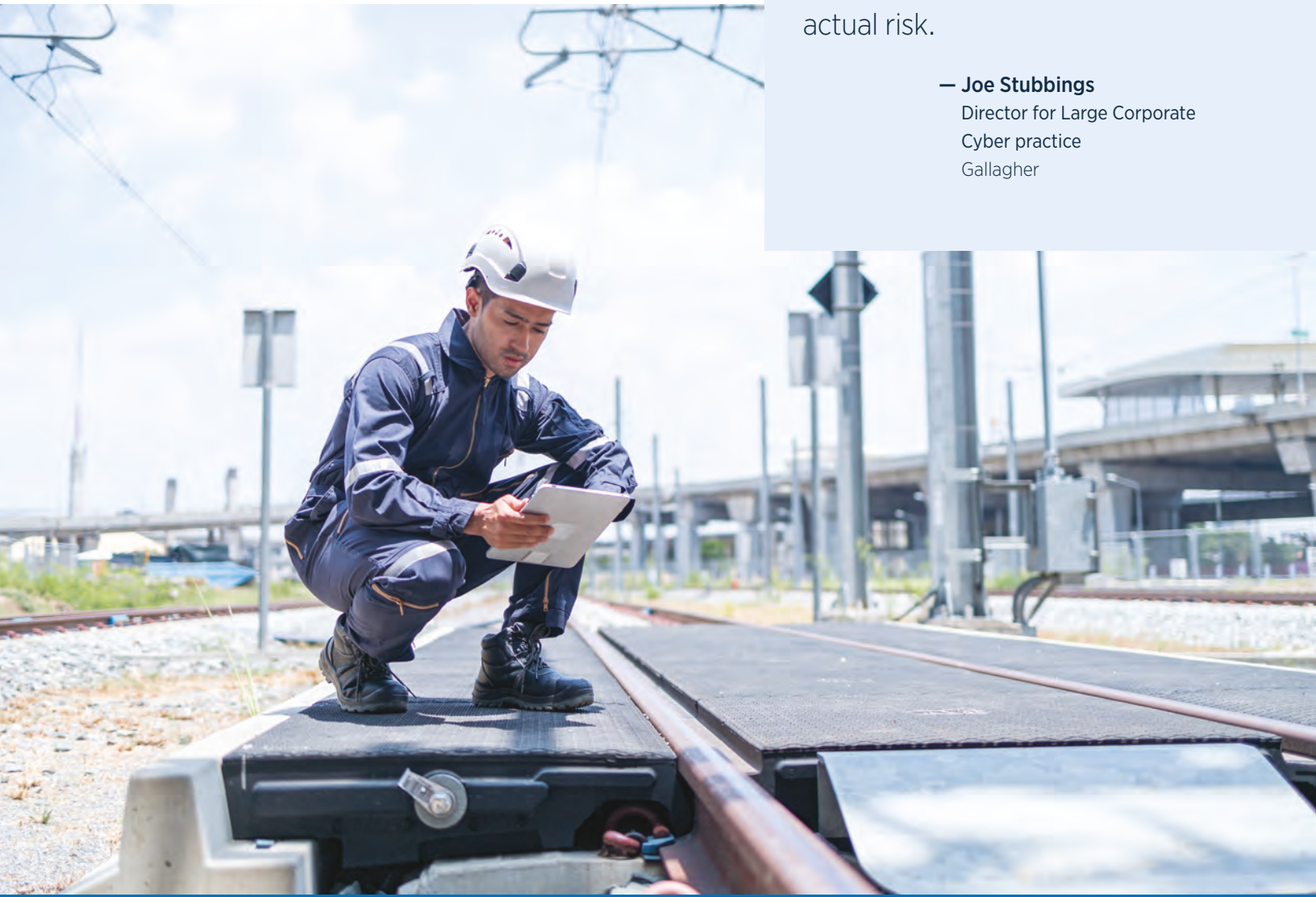
Many operators assume their P&C policies provide comprehensive protection, only to discover exclusions after an incident. It is therefore important to stress test how policies might respond by carrying out scenario planning exercises with the support of risk and insurance partners. Brokers play a key role in clarifying these details and helping organizations make informed decisions.

"It takes a knowledgeable broker to truly understand what carriers are offering, as there may be exclusions built into the policies that need to be carefully reviewed," says Woods.

"Cyber insurance goes beyond providing indemnity; it helps rail operators mitigate impacts and recover from an event more effectively. We help clients by providing clarity over their policies and the exclusions that may exist and ensure coverage aligns with actual risk," adds Stubbings.

By proactively identifying gaps and exploring tailored solutions, rail operators can build a more resilient risk management framework that reflects today's cyberthreat landscape.

> Cyber insurance goes beyond providing indemnity; it helps rail operators mitigate impacts and recover from an event more effectively. We help clients have clarity over their policies and the exclusions that may exist and ensure coverage aligns with actual risk.
>
> — **Joe Stubbings**
> Director for Large Corporate Cyber practice
> Gallagher



Assess, Quantify and Protect

Effectively managing cyber risk begins with understanding it. For railway operators, this means taking a comprehensive view of their digital ecosystem and identifying critical points of exposure.

1

Mapping exposure

A proactive first step is assessing exposure across both IT and OT environments. This includes ticketing systems, passenger data platforms, signaling infrastructure and train control systems.

Understanding how these systems interact helps prioritize cybersecurity investments and align insurance coverage.

2

Quantifying risk to inform strategy

Risk quantification is a critical tool in this process. By analyzing the potential financial impact of cyber incidents — such as business interruption, ransomware attacks or data breaches — organizations can better understand the scale of their exposure and whether current policy limits are sufficient.

Aligning insurance policies with identified risks ensures that both first-party and third-party exposures are adequately addressed.

3

Designing fit-for-purpose risk management strategies

Once risks are identified and quantified, rail operators can implement layered defenses and operational plans.

Defense layers for IT systems include technical controls such as multi-factor authentication (MFA), endpoint detection and response (EDR) and secure backup protocols to address IT system vulnerabilities. For operational planning, improvements can be made in incident response plans, ransomware readiness assessments and business continuity strategies.

These measures reduce the likelihood and impact of cyber incidents while strengthening the organization's insurability and preparedness so that if the worst happens, disruption is kept to a minimum. Underwriters expect best-in-class practices, which signal cybersecurity maturity and business resilience.

Future Trends in the Rail Industry

To keep progress on track, cybersecurity should be woven into every layer of digital transformation.

IoT and edge technology

Internet of Things (IoT) devices and edge computing are transforming rail operations by enabling real-time data collection, processing and analysis. These tools improve traffic monitoring, predictive maintenance and passenger experience.

However, each sensor, monitoring system and connected device expands the potential entry point for attackers. As Gwynne-Robinson notes, "the rail industry needs to respond with a 'secure by design' approach. This means embedding cybersecurity into the architecture of new systems to mitigate risks from the outset."

AI: An arms race between companies and cybercriminals

Artificial Intelligence (AI) promises optimized cargo tracking, traffic flow management and even autonomous train concepts. Yet, the same technology fuels cybercriminals, enabling sophisticated malware and automated attacks. "With AI, not only are attacks growing in sophistication, but also low-skilled cybercriminals are now able to create malicious software and malware to attack rail operators," explains Gwynne-Robinson.

As the technology is more integrated into operations, guidelines regarding responsible implementation, governance and ethical use need to be a priority to safeguard systems and mitigate misuse.

Autonomous rail developments

Autonomous rail technology, although still in the testing phase, is expected to reshape commuter and freight operations. Pilot programs are already underway, and broader adoption is expected soon.

As this technology matures, underwriters and insurance providers will refine models to address liability and emerging risks. Flexible, forward-looking insurance solutions will be critical to keep pace with advancements.

> The rail industry needs to respond to emerging technologies with a 'secure by design' approach. This means embedding cybersecurity into the architecture of new systems to mitigate risks from the outset.
>
> **— Nick Gwynne-Robinson**
> Consultant for Crisis and Security Strategy at Another Day
> A Gallagher company

Building Resilience Through Partnership

There is no doubt the railway industry's digital transformation is heralding a new era of efficiency and innovation, but with it comes a more complex and interconnected digital risk landscape.

For rail operators navigating this transformative phase, it's about finding the right partners and expertise to make the most of the upside while boosting cyber resilience to mitigate the downside.

With Gallagher, you can confidently navigate the digital future, protecting your assets, your people and your reputation. Contact us to learn how we can help you build a cyber-resilient rail operation.

SOURCES

[1] "Class I Rail $110m Communications Modernization Initiative Could Transform Rail Safety, Operations in 2025," *Federal Newswire*, 20 Dec 2024.

[2] "Global Cybersecurity Outlook 2025," *World Economic Forum*, 13 Jan 2025. PDF file.

AJG.com **The Gallagher Way.** Since 1927.

Gallagher

The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer financial, tax, legal or client-specific insurance or risk management advice. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Gallagher publications may contain links to non-Gallagher websites that are created and controlled by other organizations. We claim no responsibility for the content of any linked website, or any link contained therein. The inclusion of any link does not imply endorsement by Gallagher, as we have no responsibility for information referenced in material owned and controlled by other parties. Gallagher strongly encourages you to review any separate terms of use and privacy policies governing use of these third-party websites and resources.

Insurance brokerage and related services provided by Arthur J. Gallagher Risk Management Services, LLC License Nos. IL 100292093 / CA 0D69293

© 2026 Arthur J. Gallagher & Co. | PMUS106821