Cybersecurity in Transit

Preventing Damage, Disruption and Death at Critical ATC Systems, Smart Maritime Ports and Connected Railroads

By Mark Robins

Cybersecurity affects the public on many levels. The connectivity of complex software and information technology (IT) has become increasingly integral to our daily lives. As our dependency on it grows, there's been an increase in the vulnerabilities and potential attacks against it. Cybersecurity has grown out of necessity to protect these systems and the information contained within them. Exercising cybersecurity best practices is the best hope against increasing and potentially damaging cyberattacks, especially in the transportation sector.

Evolving transportation cyber-physical systems (TCPS) use computing, communications and automation power to integrate and optimize our mobility systems and infrastructure. Because of this dependence on technology, transportation systems — a major component of our critical infrastructure comprised of complex and interconnected components, subcomponents and services — are especially vulnerable to increasingly sophisticated direct and indirect cyberattacks.

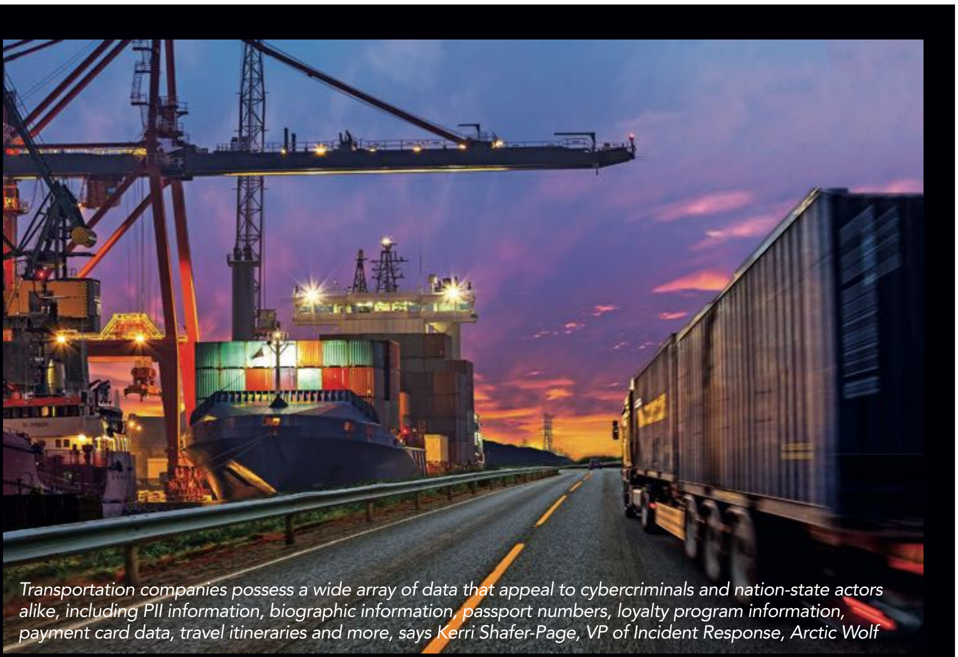
Remote hacks (whose numbers are growing) include both web-based and nearby wireless attacks. With many transportation vehicles now increasingly internet-enabled, the risk of hackers gaining access to a whole supply chain is high.

The main objective of these hacktivists, cybercriminals and nation-state actors is to exploit transportation systems. The fallout from both politically and financially motivated cyberattacks on the operational technology (OT) systems that control transportation can be particularly severe. This can involve critical air traffic control systems, smart maritime ports, connected railroads or a datacenter housing customer data. These attacks can disrupt services, threaten lives and cause significant economic damage.

The financial impact of a cyberattack's extortionate costs is real. According to IBM's "Cost of a Data Breach Report 2024" the average transportation cyberattack costs $4.4 million.

An Important Role

Cybersecurity's role in transportation is to ensure the safety and protection of critical infrastructure against threat actors aiming to exploit vulnerabilities tied to this sector. "This is a unique challenge, given that these systems feature both IT and OT, says Kerri Shafer-Page, VP of Incident Response, Arctic Wolf – North Carolina. "Cyberattacks on the transportation industry can have damaging ripple effects on other industries that rely on air, rail, truck, shipping and logistics companies to carry out their operations. Transportation companies possess a wide array of data that appeal to cybercriminals and nation-state actors alike, including PII information, biographic information, passport numbers, loyalty program information, payment card data, travel itineraries and more. Unfortunately, even as the transportation sector has pursued digital transformation improvements to make its operations more efficient, it has yet to respond to increasing cyber threats with similar urgency."

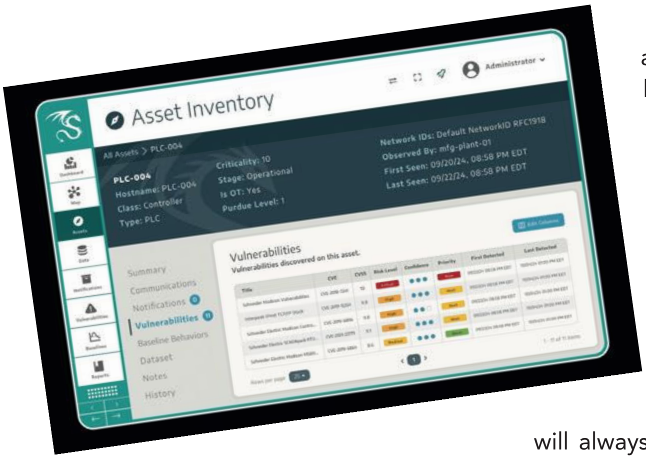


Transportation companies possess a wide array of data that appeal to cybercriminals and nation-state actors alike, including PII information, biographic information, passport numbers, loyalty program information, payment card data, travel itineraries and more, says Kerri Shafer-Page, VP of Incident Response, Arctic Wolf

Advanced transportation technologies breed more opportunities for threat actors to exploit these systems. With more tooling comes more vulnerability, more patching and more potential for missteps. "These same technological breakthroughs have expanded attack surfaces and exacerbated gaps in cybersecurity coverage," Shafer-Page adds. "As companies in the air, rail, truck, shipping and logistics spaces push to expand their reach while reducing transit times, increasing efficiencies and improving safety, they must do so while ensuring that the disruptive technologies driving their industry's innovations do not leave them exposed to cyberattacks."

Digital touchpoints run through a transportation supply chain and span infrastructure, vehicles and communication networks which creates opportunities for cybercriminals to uncover weaknesses. Kaspersky image.

Tim de Groot, general manager, Benelux, Nordics, Northwest and Francophone Africa at Kaspersky, London, explains that in our increasingly interconnected world, "The digital touchpoints running through a transportation supply chain that spans infrastructure, vehicles and communication networks creates opportunities for cybercriminals to uncover weaknesses and strike. A passenger's safety may be compromised due to a malicious attack targeting a manufacturer's operation. This can lead to significant financial and reputational damage and decision-makers within the transportation industry are hyper-aware of this. Our recent study into the automotive industry found 64% of C-Suite executives believe the automotive supply chain is currently vulnerable to attacks. What sets cybersecurity in transportation apart from other forms of cybersecurity



Asset Inventory

Administrator

All Assets > PLC-004

PLC-004
Hostname: PLC-004
Class: Controller
Type: PLC

Criticality: 10
Stage: Operational
Is OT: Yes
Purdue Level: 1

Network IDs: Default NetworkID RFC1918
Observed By: mfg-plant-01
First Seen: 09/20/24, 08:58 PM EDT
Last Seen: 09/22/24, 08:58 PM EDT

Summary
Communications
Notifications 0
Vulnerabilities 11
Baseline Behaviors
Dataset
Notes
History

Vulnerabilities
Vulnerabilities discovered on this asset.

Title	CVE	CVSS	Risk Level	Confidence	Priority	First Detected	Last Detected
[illegible]	[illegible]	10	[illegible]	●●●	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	9.8	[illegible]	●●●	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	9.8	[illegible]	●●	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	●●●	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	●●●	[illegible]	[illegible]	[illegible]

The "Dragos 2025 OT/ICS Cybersecurity Report" says nearly 10 percent of ransomware attacks against industrial organizations were in the transport sector. Dragos image.

traditional IT systems, transportation networks must balance cybersecurity with operational and physical safety. Transportation systems rely on a complex web of interconnected components that must work seamlessly together. Legacy infrastructure in transportation also makes it unique, especially within aviation and rail. These systems, not originally designed with cybersecurity in mind, make them more difficult to safeguard against modern cyber threats."

In addition to legacy issues, Rowan Macfarlane, principal industrial consultant at Dragos, Hanover, Md., explains that the emergence of ransomware is challenging our businesses. He cites the Dragos 2025 OT/ICS Cybersecurity Report, in which nearly ten percent of ransomware attacks against industrial organizations were in the transport sector. This is up from seven percent in 2023. "Further, geopolitical conflicts continue to drive national investment in cyber offensive capabilities," he adds. "We saw this with Voltzite as an example of persistence and information-gathering for future attacks through to capability development as precursors to war as observed by Electrum and Xenotime. While the number of threats is mounting, the technological competitive advantage can be squandered if cybersecurity measures aren't effective, considerate of operational requirements and appropriately managed. For businesses the challenge isn't how to secure our technology assets, but what should be done first."

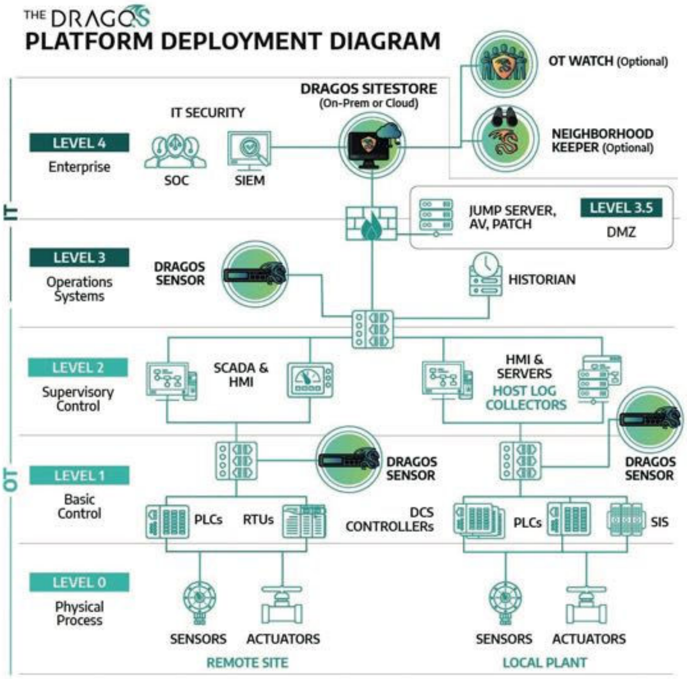
Novel Defenses, Reactive Capabilities

Cybercriminals attacking the transportation (or any other high-tech industry) will always adapt and evolve as needed to achieve their goals, which Shafer-Page explains means sometimes using low-tech methods of social engineering and sometimes means using cutting-edge, advanced zero-day exploits. Either way, "They're unencumbered by laws, certain ethical standards or institutional planning horizons. The lesson here is that preventative measures alone are insufficient for transportation companies' cybersecurity posture."

The ways that cybersecurity threats in transportation are handled today have clearly changed. What was once a matter of installing antivirus software and following basic IT protocols has now evolved into a relentless battle against sophisticated cyber threats, complex coding and continuous attacks. Intelligence reports and real-time threat warnings have become essential in helping businesses protect their operations, products and intellectual property. Nowhere is this more critical than in the transportation sector where a cyberattack can put passenger safety at direct risk. The industry has had to shift its mindset, recognizing that cybersecurity is no longer just about protecting data but about ensuring the safety and integrity of entire transport networks.

According to de Groot, real-time intrusion detection systems (IDS) can monitor networks and onboard systems, allowing operators to identify and mitigate potential cyber incidents before they escalate into serious disruptions. "Secure communication protocols are also evolving, ensuring that critical data exchanged between central hubs and the aircraft or train remains protected from unauthorized access."

Artificial intelligence (AI) and machine learning is now being embedded into cybersecurity frameworks. As the industry moves toward more proactive threat detection, de Groot explains that anomalies and potential breaches can be identified in real time and neutralized before they pose a risk. "In aircraft specifically, avionics systems are using hardware-based security modules, preventing unauthorized interference and reinforcing the resilience of aircraft



Dragos says their platform offers comprehensive OT network visibility and security monitoring, enabling customers to identify and inventory assets, manage and prioritize vulnerabilities and detect and respond to threats. Dragos image.

against cyberattacks."

Shafer-Page stresses that, "Defenders must build and maintain a foundation of fundamentals and continually adapt and evolve their security posture such that, over time, those novel defenses are integrated into the new normal. But defenders must also augment these proactive measures with reactive capabilities designed to quickly and effectively detect and respond to attacks that break through outer defenses, as well as risk-transfer measures."

Dragos is focused on protecting OT environments such as systems like baggage handling, weather management, security and surveillance and facility management, particularly lighting control systems. The Dragos Platform offers comprehensive OT network visibility and security monitoring, enabling customers to identify and inventory assets, manage and prioritize vulnerabilities and detect and respond to threats. The Platform is codified with OT-specific threat analytics and insights from a team of OT cybersecurity practitioners. Dragos WorldView threat intelligence delivers in-depth visibility of emerging threats targeting industrial environments globally, and the defensive recommendations to combat them.

A Good Cybersecurity Strategy

A comprehensive approach is essential for developing a strong cybersecurity strategy. This starts with a thorough situation analysis across the company, which can help an organization identify any risks they may be vulnerable to in its software, hardware and networks. Security measures to combat attacks must be multilayered throughout the organization due to the intricacies of transportation.

"Organizations should create a clear incident response plan, ensuring that any cyber incident can be swiftly contained and resolved to minimize disruption," de Groot says. "Regular system updates, continuous staff training and a proactive approach when it comes to collaborating with other industry players all enhance an organization's security position."

Organizations should deploy strong security tools like managed detection and response (MDR), which can identify and mitigate suspicious activity in real-time. Everyone should be deploying multi-factor authentication as well, according to Kerri Shafer-Page of Arctic Wolf.

Shafer-Page explains that the same cybersecurity strategy advice she gives to transportation companies applies to all companies. "Organizations should deploy strong security tools like managed detection and response (MDR), which can identify and mitigate suspicious activity in real time. Everyone should be deploying multi-factor authentication as well. Besides those things, best practices include always patching vulnerabilities as quickly as possible and ensuring you're deploying a strong employee security training program to educate your workforce about suspicious activity."

Many standards and frameworks exist that can help organizations with cybersecurity, including detailed guidance on controls and network architecture principles. But Macfarlane cautions that often, these frameworks are geared toward IT networks and don't give enough consideration to the operational requirements needed to administer or implement best practices in an organization. Instead, he explains the SANS 5 ICS Cybersecurity Critical Controls pioneers a threat-led approach for defenders.

The five Critical Controls include:

- Developing an ICS incident response plan.
- Implementing a defensible architecture, including proper network segmentation.
- Continuous ICS network visibility monitoring.
- Using secure remote access.
- Risk-based vulnerability management that understands OT environments to allow informed decisions about whether to patch vulnerabilities, mitigate impacts, and monitor for exploitation.

Mcfarlane explains that each of the five controls should be evaluated regularly, particularly as new threat intelligence becomes available, focusing on doing the simple controls thoroughly and effectively. This allows defenders to measurably address the most significant and applicable risks to the business.

The federal government understands the importance of cybersecurity strategies. In 2022, it passed the Infrastructure Investment and Jobs Act, which included $2 billion for the Department of Transportation to expand its cybersecurity initiatives. State, local and private agencies can address current vulnerabilities such as ransomware, aging infrastructure, insufficient security assessments and vehicle links to IT networks, and prepare to foster emerging opportunities such as security by design, new research and intelligent automation. TSI