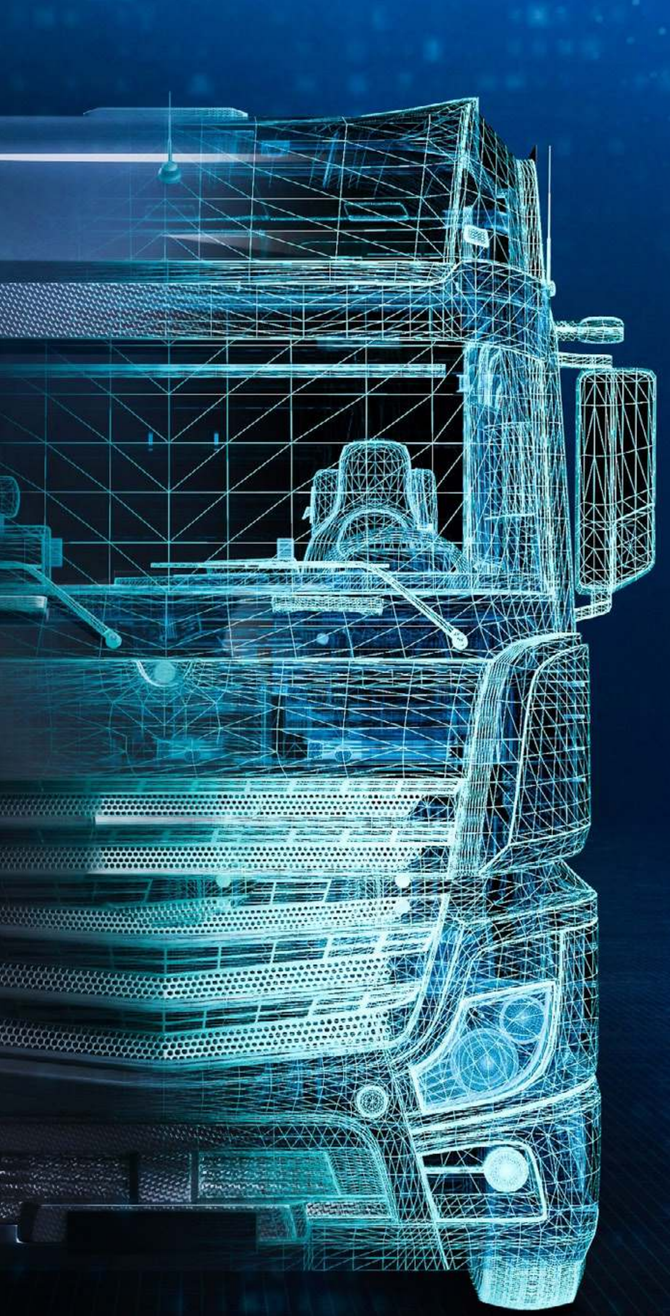


2025 Trucking Cybersecurity Trends Report

NMFTA™
National Motor Freight Traffic Association, Inc.

TABLE OF CONTENTS

INTRODUCTION

The trucking industry is no stranger to disruption, and as we look toward 2025, cybersecurity is poised to become one of the most pressing challenges fleets will face. With the rise of artificial intelligence (AI)-enhanced phishing campaigns, increasingly sophisticated cyber-enabled cargo theft, and the rapid evolution of machine learning-based defense mechanisms, the landscape is shifting in ways that demand attention.

Threat actors are becoming more adept at exploiting vulnerabilities faster and more intelligently, leveraging advanced tools that make phishing, malware creation, and impersonation scams harder to detect and prevent. At the same time, cybersecurity solutions are evolving to meet these challenges, from enhanced threat detection to widespread adoption of Zero-Trust architectures and application programming interface (API) security.

In this report, we'll explore the key trends that will define trucking cybersecurity in 2025, highlighting both the opportunities and threats that lie ahead. For industry leaders, staying informed and proactive in the face of these changes is critical—not only to protect their operations but to ensure the future resilience of their fleets.

Now, let's dive into the critical cybersecurity developments that trucking professionals must be prepared to address in the year ahead.

TRUCKING CYBERSECURITY TRENDS FOR 2025

What's New in Phishing

Traditional and AI-Enhanced Phishing

Phishing is not a new technique. It has long been one of the most successful attack vectors leveraged by threat actors to gain initial entry into an organization. However, 2025 will see significant increases in the efficiency and accuracy of phishing attempts, making traditional methods of detection less effective. AI tools, and the advancements expected in 2025, will act as force-multipliers for threat actors as they craft increasingly sophisticated and believable phishing campaigns.

Delayed Phishing

In addition to traditional phishing techniques used to deliver malicious content, 2025 will see an increased utilization of advanced evasive techniques such as delayed phishing to avoid detection by even the most advanced secure email gateways (SEGs) and other email security tools. This will require the trucking industry to focus on both improved detection and response tools for email security and increased cybersecurity training for their employees to ensure awareness of the risks that email poses to the organization.

Increased Impact from AI and Machine Learning

AI and machine learning (ML) will continue to play a crucial role in both defense and attack. Expect more advanced threat detection, automated responses, and predictive analytics to identify vulnerabilities before they can be exploited.

AI Used by Threat Actors

Threat actors will continue to increase their use of AI to mount ever-more sophisticated and targeted phishing attacks. AI is also continuing to lower the bar to entry for the creation of malware and increasing the speed with which bad actors can craft exploits for vulnerabilities once they are published. The rapidly improving quality and accessibility of AI generated deep-fake video and voice recordings will increase the likelihood of impersonation scams and vishing attacks facilitated by AI tools in 2025.

AI Used by Cybersecurity Defense

Machine speed, AI-enhanced detection and response capabilities will continue to improve and expand in their scope of application across the cyber-defense ecosystem. We expect to see improved anomaly detection and increases in AI-powered automation in cybersecurity tools. As threat actors craft more believable phishing emails with fewer of the traditional tells, AI will become a valuable partner in the loop to facilitate detection of these craftier campaigns.

Zero-Trust Architecture Adoption Increases

The adoption of Zero-Trust architecture will become more widespread. This approach assumes that threats could be both external and internal, so it enforces strict verification processes and least privilege access controls. With increasingly sophisticated impersonation methods, the rise of efficient phishing campaigns increases the likelihood of credential theft. As a result, pivoting to an architecture based on proof of identity through additional security controls and the verification of both individuals and devices will become paramount.

API Security

Application programming interface (API) security continues to be a top area of focus looking ahead to 2025. While the move toward Zero-Trust principles is the core of API security design, the continued evolution of AI and ML technologies will also bolster the API security toolset in many organizations.

Stricter authentication mechanisms are becoming standard practices, but the focus is shifting to adaptive and continuous authorization strategies that leverage behavioral analytics (with the help of AI and ML) to monitor for anomalies in API traffic in real time.

Cyber-Enabled Cargo Theft

With advances in large language models (LLMs) and other AI technology, phishing campaigns are increasingly difficult to detect. Deferred malicious links also continue to pose threats in phishing and credential theft schemes. Readily available consumer tools now allow for easy modification of bills of ladings to hide pilfering with an ever-decreasing bar of entry. These techniques, along with website poisoning and lookalike domains will continue to drive increased levels of cyber-enabled strategic cargo theft in 2025.

Threats to Assets and IoT

Fleets are going to continue to deploy Internet of Things (IoT), especially on trailers, and with these devices come risks that must be proactively managed. In 2025, fleets will be well-advised to observe and apply best practices from the world of industrial control systems (ICS) by sourcing and deploying products with good cybersecurity controls baked into their design, but also taking responsibility for deploying and configuring them with cybersecurity as a priority.

While original equipment manufacturer (OEM) vendors are beginning to prioritize security in their devices as well as increases in standardizations (Society of Automotive Engineers (SAE) / International Organization for Standardization (ISO)) that relate directly to heavy commercial vehicles and their onboard and connected systems, this does not solve the issues of a lack of transparency into devices and a lack of user control of core security settings. Expect increasing pressure from the trucking and supply chain industry to move the OEM community toward increased transparency and continued focus on Secure by Design architecture.

Enhanced Privacy Regulations

As data privacy concerns grow, we expect more stringent regulations and compliance requirements globally. Companies will need to stay ahead of these regulations and ensure their practices align with them.

The North American trucking industry will need to be aware of the changing privacy landscape and the ways that privacy regulations may differ between states, as well as between the United States (U.S.), Canada, and Mexico. There are already differing privacy regulations that have become law in multiple U.S. states, requiring careful handling of customer and employee data to ensure compliance with all applicable regulations. NMFTA anticipates additional states will begin or complete the process of enacting some form of consumer protection, or AI-related privacy regulation in 2025. Adhering to the highest common denominator in privacy regulation will be key to ensuring compliance across the industry.

PREDICTIONS FROM ACROSS THE CYBERSECURITY INDUSTRY

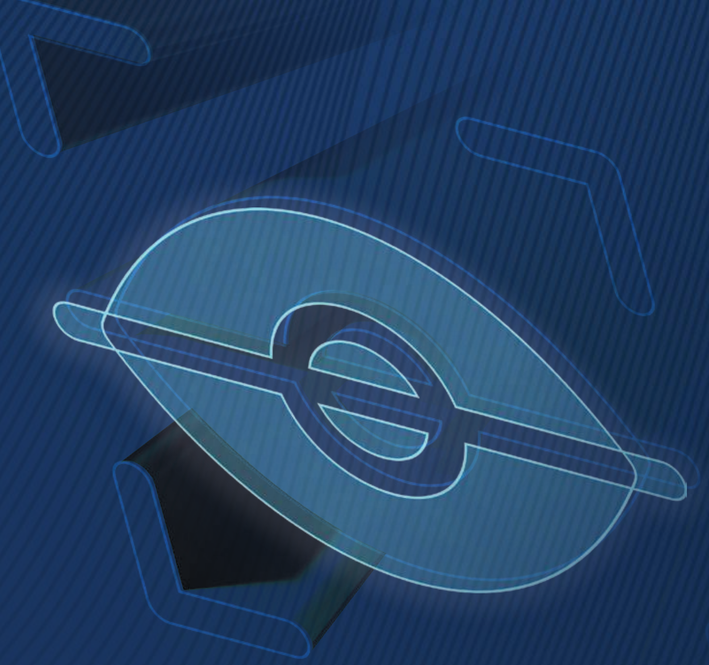
Forrester

Litigation

The overall percentage of companies facing class-actions lawsuits is at a 13-year high. "*Historically, cyber regulations have not gone far enough to protect customers and employees, [this encourages] these same people to pursue class-action lawsuits and to seek damages*" states Cody Scott, senior analyst for Forrester. He goes on to say that Forrester expects breach-related class action costs will be on the rise; "*possibly surpassing regulatory fines by as much as 50%.*"

Regulation

Forrester is anticipating that due to the increased awareness of software supply chain vulnerabilities among government, there will be increased pressure on western governments to regulate or restrict specific third party and open-source software components that are deemed to pose a risk to national security. They predict that this may become a top priority in 2025 for many western nations.



Deprioritized Use of GenAI by CISOs

Forrester is taking a different stance on the use of generative AI (genAI) tools in cybersecurity in 2025 than many organizations, they predict a 10% reduction in the prioritization of genAI by global chief information security officers (CISOs).

> *"According to Forrester's 2024 data, 35% of global CISOs and CIOs consider exploring and deploying use cases for genAI to improve employee productivity as a top priority. The security product market has been quick to hype genAI's expected productivity benefits, but a lack of practical outcomes is fostering disillusionment. The thought of an autonomous security operations center using genAI generated a lot of hype, but it couldn't be further from reality. In 2025, the trend will continue, and security practitioners will sink deeper into disenchantment as challenges such as inadequate budgets and unrealized AI benefits reduce the number of security-focused genAI deployments."*[1]

1 Scott, C. (2024, October 1). *Predictions 2025: Security and risk pros will brace for regulations and resilience.* Forrester. https://www.forrester.com/blogs/predictions-2025-cybersecurity-risk-privacy/

Gartner

Increased Need for Cloud Security Solutions

2025 will see a continuation of the shift to the cloud, which Gartner analysts predict will lead to increases in the cloud security solutions space. They predict that the combined market for cloud access security brokers (CASB) and cloud workload protection platforms (CWPP) may reach an estimated $8.7 billion in 2025, up from $6.7 billion in 2024.

Cybersecurity Skills Shortage to Continue

Gartner predicts that the shortage of skilled cybersecurity talent will continue to pressure organizations to onboard security services and managed service providers in 2025.

"The global skills shortage in the cybersecurity industry is a major factor driving investment in the security services market (security consulting services, security professional services and managed security services) which is expected to grow faster than the other security segments."

Increased Security Requirements Surrounding GenAI

"The adoption of AI and generative AI (GenAI) continues to increase investments in security software markets like application security, data security and privacy, and infrastructure protection. Through 2025, GenAI will trigger a spike in the cybersecurity resources required to secure it, leading to an expected 15% increase on security software spending (see Table 1).

Since the release of GenAI, attackers are increasingly employing tools along with large language models (LLMs) to carry out large-scale social engineering attacks, and Gartner predicts that by 2027, 17% of total cyberattacks/data leaks will involve generative AI."

Table 1. Information Security End-User Spending by Segment, Worldwide, 2023-2025 (Millions of U.S. Dollars)

Segment	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)	2025 Spending	2025 Growth (%)
Security Software	76,574	13.6	87,481	14.2	100,692	15.1
Security Services	65,556	13.6	74,478	13.6	86,073	15.6
Network Security	19,985	6.2	21,912	9.6	24,787	13.1
Total	**162,115**	**12.7**	**183,872**	**13.4**	**211,552**	**15.1**

Source: Gartner (August 2024)[2]

2 *Gartner Forecasts Global Information Security Spending to Grow 15% in.* (2024, August 28). Gartner. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

CONCLUSION

2025 will bring improvements in cybersecurity across the trucking and supply chain industry, and it will also bring new and evolving threats. The trends highlighted in this report reinforce the need for a proactive approach to risk management and cybersecurity. As cybersecurity professionals and business leaders, it is critical that we remain vigilant and understand that cybersecurity is a practice that requires flexibility and adaptability, and one that is vital to the success of our operations. Good cybersecurity ensures the resiliency of our critical industry.

The National Motor Freight Traffic Association, Inc. (NMFTA)™ will be vigilant throughout 2025 about following these issues and sharing our findings with the industry through whitepapers, webinars, live speaking engagements, and blogs. This effort will culminate, as always, with our annual three-day Cybersecurity Conference, which will take place on October 26-28, 2025, in Austin, TX.

ABOUT US

The NMFTA is a non-profit organization that represents the interests of less-than-truckload (LTL) carriers, by providing critical services to the industry in the form of classification standards, identification codes, digital operation standards, and support for cybersecurity. The NMFTA has also been a leader for more than a decade in trucking cybersecurity research.

Learn More: nmfta.org

Follow Us:

NMFTA CYBERSECURITY RESOURCES

Events

NMFTA hosts monthly webinars and an annual Cybersecurity Conference every Fall.

Visit nmfta.org/nmfta-events

Research and Whitepapers

Explore NMFTA's research and whitepapers for insights on key cybersecurity topics, trends, and strategies.

Visit nmfta.org/cybersecurity/cybersecurity-research/