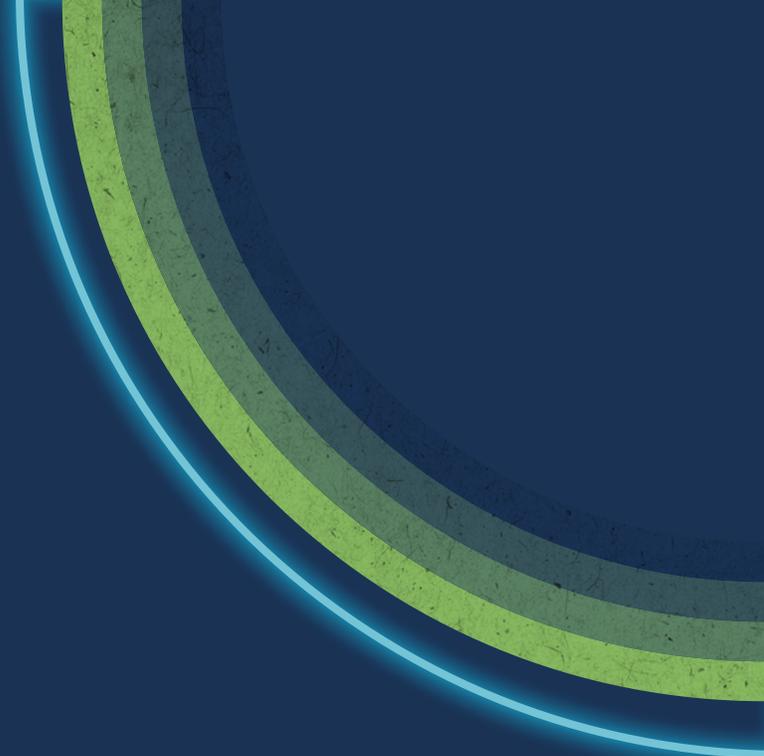


2026

TRANSPORTATION INDUSTRY CYBERSECURITY TRENDS REPORT





“

The convergence of traditional cargo theft, cybercrime, and operational disruptions has transformed trucking cybersecurity from an IT issue into a full-spectrum operational resilience challenge.

”

TABLE OF CONTENTS

Executive Summary	4
2025 in the Rearview & The Road Ahead for 2026	5
Sophistication and Specialization of Cybercrime in Trucking	10
People, Processes, and Technology Trends	14
Digital Asset Cybersecurity Trends	18
Physical Asset Cybersecurity Trends	22
Emerging Technology Cybersecurity Trends	25
Privacy Laws, Regulatory Landscape, Geopolitical Influences and Impacts	29
Conclusion	33
NMFTA Cybersecurity Resources	34
NMFTA Cybersecurity Best Practices Guidebooks	34
NMFTA Cargo Crime Reduction Framework	34
NMFTA Cybersecurity Webinar Series	35
Annual NMFTA Cybersecurity Conference	35
About Us	36
Appendix	37
Industry, Cybersecurity & Technical Acronyms	37
Transportation & Regulatory Acronyms	38
References	39

EXECUTIVE SUMMARY

Several positive indicators for the growth of cybersecurity maturity in the transportation sector surfaced in 2025. The sector showed significant signs that targeted, role-based cybersecurity awareness training is now considered a part of core operational preparedness. Fleets and logistics companies that invested in ongoing social engineering awareness training and phishing simulations saw measurable reductions in successful social-engineering incidents. The practice of sharing cybersecurity threat intelligence, indicators of compromise, and lessons learned also gained significant momentum across the sector in 2025.

On the other side of the equation, the past year was also a year in which social engineering, identity compromise, and supply-chain exploitation accelerated as the dominant drivers of both financial loss and systemic risk across the transportation sector. While increasing adoption of artificial intelligence (AI) and AI-enabled technologies across the sector has served to boost operational efficiency and aid in enhanced detection and response capabilities, it has also introduced significant new security challenges.

Throughout 2025, cybercriminal activity demonstrated a new degree of sophistication and increased specialization. Groups that once operated independently formed specialized alliances, increasing both the speed and efficiency of cyberattacks on organizations across the sector. Entering 2026, the North American transportation sector faces the most complex and dynamic cyber threat environment in its history. The convergence of traditional cargo theft, cybercrime, and operational disruptions has transformed trucking cybersecurity from an IT issue into a full-spectrum operational resilience challenge.

Ransomware and extortion by means of data exfiltration, frequently deployed through the weaponization of legitimate remote access tools, remained a significant threat to the transportation sector even as state-sponsored actions targeting critical infrastructure networks and devices across the nation saw sustained and elevated activity.

The transportation sector's security posture in 2026 must extend far beyond technical controls. Effective preparedness requires the integration of cybersecurity into every layer of the business. From intelligence gathering and sharing through response and recovery actions, the next phase of resilience will hinge on convergence; on treating physical security, operation security, and cybersecurity as components of a single, holistic security strategy. This has become the requisite baseline in organizational resilience planning.

**2025 IN THE
REARVIEW
& THE ROAD
AHEAD FOR
2026**



Social engineering remained the leading risk facing the transportation industry in 2025. Cybercriminals and cargo thieves leveraged both traditional deception and new technologies to conduct highly targeted campaigns against carriers, brokers, and shippers. These attacks served as the entry point for ransomware, data theft, and extortion schemes, and increasingly formed the foundation for cyber-enabled cargo crimes. Across the sector, the correlation between digital compromise and physical theft is now unmistakable. Cyber intrusion often precedes or directly enables theft of freight.

Throughout 2025, cargo crime trends remained elevated. CargoNet reported that in Q3 2025, cargo theft claims reached \$111.88 million (Verisk, 2025). As staggering as this number is, it is well understood that reported cargo crimes only represent a small percentage of total cargo crimes experienced across the sector due to widespread underreporting. While traditional hotspots such as California and Texas contributed to year-over-year increases, the most dramatic growth occurred in the New York City metropolitan area, specifically New Jersey and eastern Pennsylvania (up 110% and 33%, respectively). Analysts attributed these spikes to the adoption of cybercrime tactics by organized criminal networks who leveraged social engineering to impersonate carriers, hijack Federal Motor Carrier Safety Administration (FMCSA) accounts, and manipulate load tenders and other dispatch documentation. The result is a seamless blend of cybercrime and physical theft, where stolen credentials, fake identities, and compromised systems have facilitated physical theft of cargo at unprecedented levels.

This correlation was reinforced by a series of 2025 investigations into organized theft networks that combined phishing, credential harvesting, and fraud at scale. Bad actors used AI-generated emails, deep-fake voice calls, and spoofed dispatch updates to misdirect shipments or extort payments through fraudulent detention or lumper fees. In many cases, attackers used business email compromise (BEC) to take over legitimate communication channels and fraudulently book loads, deliver false pickup authorizations, change banking information, or change delivery instructions. These examples demonstrate the extent to which digital deception has become embedded in the cargo crime ecosystem.

At the same time, the general cybersecurity threat landscape for the transportation sector also evolved in both sophistication and tempo throughout 2025. ReliaQuest, cybersecurity company that provides a security-operations platform and managed detection/response services to large enterprises, found that the average breakout time (the period between initial compromise and lateral movement) fell to only 18 minutes by the end of Q3, underscoring the speed with which modern attackers operate (ReliaQuest, What's trending: Top cyber attacker techniques, June-August 2025, 2025). Many of these intrusions leveraged legitimate remote management and file transfer tools already present in victim environments to encrypt or exfiltrate data or extract operational details.

The average breakout time fell to only 18 minutes—faster than human defenders can respond manually.

Supply-chain compromise emerged as another critical risk vector as highlighted in multiple high-profile incidents in 2025. Each incident exposed the same structural weakness: The transportation sector's reliance on a web of software-as-a-service (SaaS) providers and integration partners. Adversaries are exploiting this trust model, compromising a vendor or a platform and pivoting into multiple connected fleets, shippers or brokers. This concentration risk represents not just an IT risk, but a systemic supply chain vulnerability.

Ransomware remained the most financially damaging cyber threat for most individual victims throughout 2025. The fragmentation of groups following the decline of LockBit and RansomHub led to an explosion of smaller, specialized operations. More than 80 distinct ransomware brands/groups were observed by Q3. Many of these newer groups were observed targeting smaller and mid-sized fleets in the transportation sector. These victims often had smaller IT teams

and limited security budgets, making them an appealing target to bad actors. The rise of AI-driven cyber threats further amplified these challenges. Generative AI tools now enable attackers to craft flawless phishing emails, replicate executive's voices, and produce counterfeit documentation nearly indistinguishable from legitimate shipping documents. This use of AI for both deception and attack automation has significantly shortened response windows.

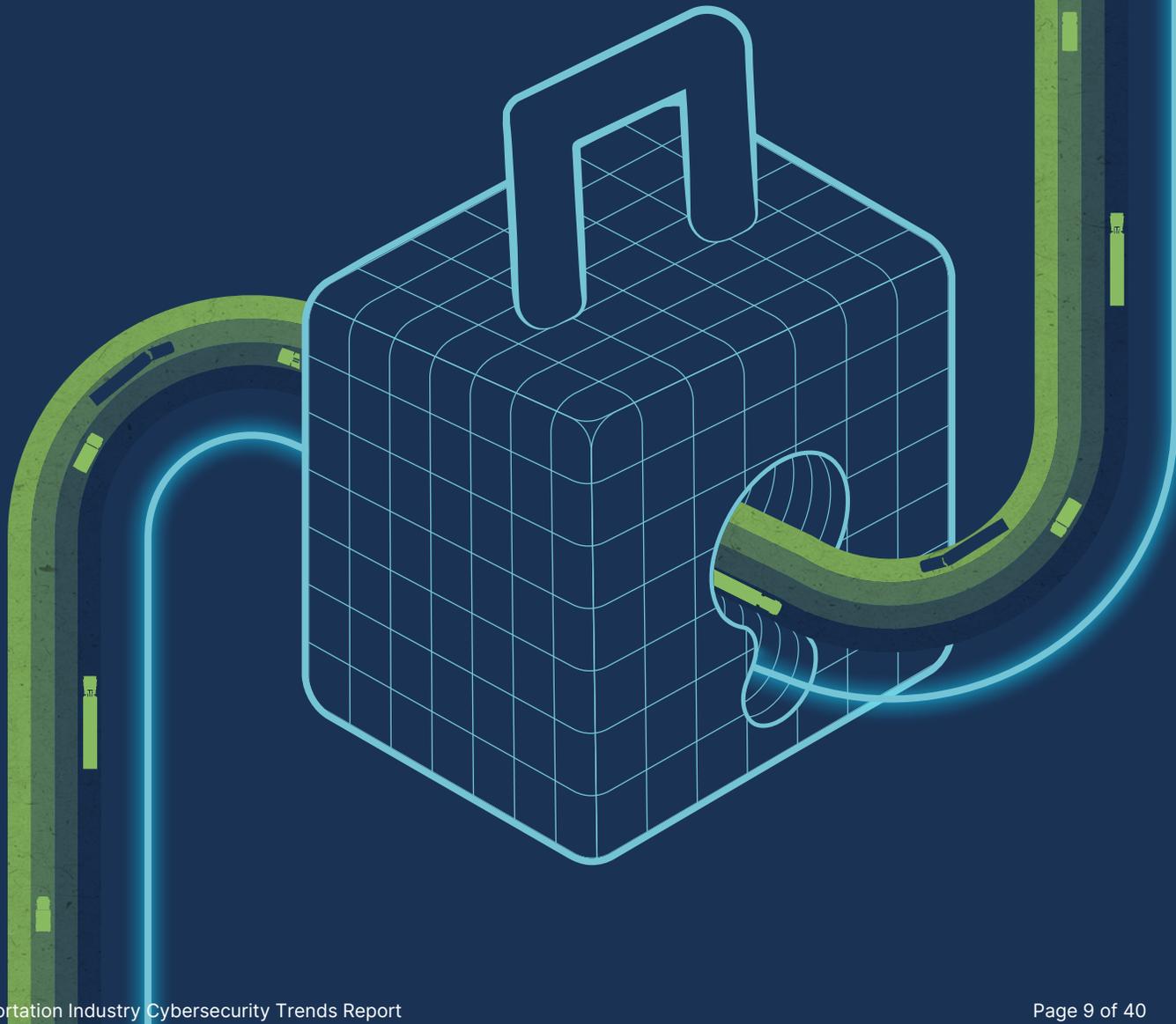
Application programming interface (API) security concerns remained elevated throughout 2025 with clear indicators that both improperly secured and legacy APIs are being regularly exploited. Leaked API credentials continue to be a significant risk as well. Ensuring that the API design process follows secure-by-design principles, legacy APIs are secured or replaced, and API credentials are carefully managed to reduce the risk of exposure will be critical in 2026.

Despite this heightened risk environment, there are encouraging trends. Industry collaboration through the National Motor Freight Traffic Association, Inc.'s (NMFTA)[™] cybersecurity initiatives, including the [Cybersecurity Best Practices Guidebooks](#), [Vendor Risk Assessment Framework](#), and [Cargo Crime Reduction Framework](#), has begun to influence operating norms. Awareness training, Electronic Logging Devices (ELDs) and telematics device validation, use of multi-factor authentication (MFA), and cybersecurity incident response preparedness are increasingly seen as core competencies of fleet operations rather than optional security controls. Additionally, transportation associations, industry stakeholders, law enforcement, and government agencies are promoting a shared defense model that treats cybersecurity as an essential component of supply-chain continuity.

These positive trends will continue in 2026 given the demonstrated appetite and commitment across the transportation sector for meaningful collaborations and shared collection, fusion and dissemination of cybersecurity, operational security, and physical security intelligence. 2026 will ring the new year with several emergent developments across the sector, while continuing the refinement of existing trends. These include:

1. Continued specialization of cybercrime groups will be coupled with collaborative efforts that further increase the efficiency of cyberattacks.
2. Attack speed and automation will continue to outpace human-scale response capacity, making continuous monitoring and automated detection and response capabilities essential.
3. Ransomware and extortion schemes remain fragmented. Exfiltration will gain prominence over encryption as the primary means of extortion.
4. Social engineering will remain the single most effective attack vector, further enhanced by sophisticated AI-enabled, industry specific tactics and techniques.
5. Cyber-enabled cargo crimes will continue rising as organized criminal groups further refine their merging of traditional theft operations with offensive cyber capabilities.
6. The weaponization of legitimate administrative tools will increase complicating detection and response efforts while requiring more carefully tuned defenses.
7. Supply-chain trust exploitation will accelerate as adversaries increasingly seek to weaponize interconnected SaaS platforms, telematics providers, Global Positioning System (GPS) devices, cloud environments, and transportation management systems (TMSs).
8. AI will remain a transformative force in the industry, aiding both attackers and defenders while facilitating significant changes to operational processes.
9. Regulatory emphasis on incident reporting, data privacy, and supply-chain cyber assurance will intensify, driven by new federal mandates and insurance market pressures.

SOPHISTICATION AND SPECIALIZATION OF CYBERCRIME IN TRUCKING



The past year was clearly marked by the maturation of many organized cybercrime operations, including those who are targeting the North American transportation sector. An attack environment that used to be primarily populated by opportunistic credential theft and ransomware deployments has evolved into a structured, corporate-like ecosystem with distinct areas of specialization, efficient division of labor, and coordination between bad actors. Groups that once operated independently, such as ransomware operators, data brokers, social engineers, and identity fraud specialists, are now collaborating with unprecedented efficiency. The resulting ecosystem rivals the complexity of legitimate transportation and logistics networks. It is decentralized, modular, and highly adaptive.

ReliaQuest's intelligence reporting on the "professionalization of cybercrime" found that modern threat groups are operating as full-scale enterprises, complete with recruiting pipelines, training programs, and specialized departments focusing on functions such as access brokering, AI-driven reconnaissance, and financial operations (ReliaQuest, ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report, 2025). Instead of relying on generalized hackers, these organizations now recruit domain experts who understand industry-specific technologies such as TMSs, telematics, and cloud-based applications. This trend signals a structural shift in the ways that adversaries operate. Bad actors now view the transportation supply chain not as a peripheral target, but as a mature, high-value target domain that is worth investing significant time, resources, and dedicated expertise due to the high potential reward for their efforts.

Evidence of targeted specializations is prevalent across the bad-actor landscape. Groups like Scattered Spider, ShinyHunters, and multiple LockBit affiliates adopted distinct roles across the attack lifecycle. Initial access brokers focused on harvesting credentials through phishing or other social engineering attacks. In the transportation industry, these attacks often include impersonation of dispatchers and brokers in addition to the more broadly observed use of IT helpdesk and executive impersonations seen in all industries. Once inside, ransomware actors like Akira, Clop, and Play were engaged to execute data exfiltration, encryption and extortion, while specialized monetization teams handled ransom negotiations and cryptocurrency laundering. Each participant extracts profit from their stage of the attack, with no single group needing to develop all the skills required to master the entire attack cycle.

This more modular structure increases both the speed and the impact of attacks. The average time between initial access and full system compromise continues to decrease, from days or hours to mere minutes. Once intrusion begins, lateral movement and data exfiltration now occur faster than human defenders can respond manually. Attacks observed in 2025 predominantly relied less on exotic zero-day exploits than on efficiency and the exploitation of human weaknesses and process gaps. Attackers are increasingly leveraging legitimate administration tools, exploiting human error, and automating the attack process.

This specialized collaboration trend has further reinforced the "cybercrime-as-a-service" model. Access brokers now sell verified credentials on dark web

marketplaces, often bundled with other internal data, such as shipping lanes, billing templates, driver records, and insurance information stolen in prior breaches. For as little as a few hundred dollars, attackers can purchase ready-to-use entry points into a target company's networks (complete with active user credentials). This economy of scale has allowed even low-skill actors to execute sophisticated attacks using pre-built tools and purchased credentials.

Particularly concerning in 2025 was the growing crossover of Tools, Tactics and Procedures, (TTPs) between cybercrime syndicates and organized cargo crime rings. Intelligence collected throughout 2025 highlighted multiple cases in which traditional cargo crime groups employed cybercrime TTPs to identify, track, and intercept cargo shipments. Cyber-enabled cargo thieves infiltrated dispatch systems, fraudulently booked loads by impersonating legitimate carriers, and spoofed or jammed GPS signals to facilitate physical theft of shipments. This evolution of tactics underscores the blurring of the boundaries between cyber intrusions and physical crimes in the transportation sector.

Formal criminal alliances have also been observed in 2025. Joint operations between ShinyHunters (known for exploiting cloud-based CRM systems) and Scattered Spider (known for social engineering tactics) show how bad actors are effectively combining technical exploitation with psychological manipulation. In partnerships like this, one group gains initial access via credential compromise while another leverages that toehold to deploy ransomware, steal data, or manipulate business communications

to facilitate other crimes (ReliaQuest, ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report, 2025). This specialization-driven collaboration dramatically increases success rates, particularly in industries dependent on rapid trust-based exchanges, such as the trucking industry.

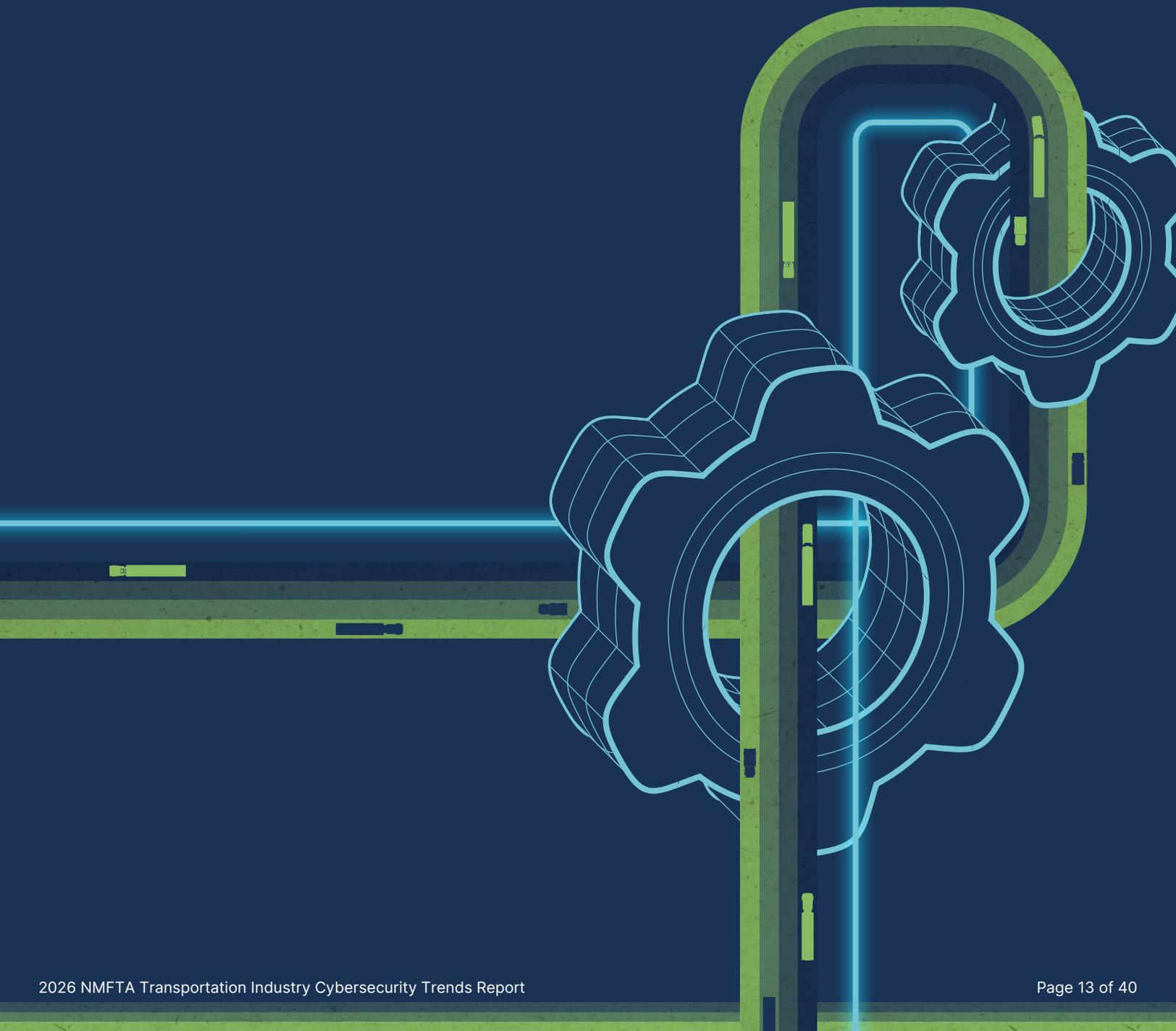
The recruitment of technical specialists, in areas including but not limited to AI, Internet of Things (IoT), blockchain, accounting, business process understanding, cloud expertise and industry specific software, has further accelerated this evolution. Bad actor groups have actively recruited or coerced former IT professionals, often offering significant financial incentives in the form of cryptocurrency payments. Recruitment ads posted on encrypted forums and social platforms specifically target individuals familiar with the systems and software related to intended target organizations. These tactics mirror what has historically been seen in state-sponsored cyber operations, with specialists from the private sector and criminal operations being leveraged to complete complex offensive cyber operations.

Enhanced persistence capabilities and repeated attacks on victims once they are compromised will be increasingly seen across the sector. Rather than deploying one-time ransomware payloads, bad actors now leverage persistent access and stolen credentials to generate continuous revenue streams through long-term access and repeated data theft and extortion operations. ReliaQuest analysts recently documented multiple cases where bad actors maintained access for months, exfiltrating operational data incrementally before triggering an overt

ransomware attack. The stolen information was then leveraged for fraud, identity theft, phishing campaigns, and extortion efforts. Throughout 2026, it is likely a continued decrease in the instances of traditional encryption-based ransomware deployments will be observed, with bad actors instead focusing more on data theft for extortion due to the higher likelihood of successful exfiltration rather than attempting encryption and risking detection.

As cybercrime groups continue to specialize and expand their bench of expertise through active recruiting and collaboration between groups, trucking and logistics operations should anticipate more disciplined and businesslike adversaries. The implications for defenders are clear: Reactive cybersecurity is no longer acceptable. The industry must adopt proactive and coordinated defensive structures, integrating intelligence gathering, analysis and distribution, continuous monitoring, and cross-functional coordination between IT, operations, and compliance teams. Only by outpacing the sophistication and adaptability of the adversaries can fleets reduce the speed, impact, and success rate of modern cybercriminals.

PEOPLE, PROCESSES, AND TECHNOLOGY TRENDS



The current operating environment in the transportation sector demonstrates that cybersecurity risks have become inseparable from day-to-day business risks. While technology continues to deliver efficiency gains through ELDs, telematics, cloud-based management platforms, and AI-enabled tooling, these same systems are regularly exploited by attackers. Cyberattacks observed across the sector reveal an evolution from isolated incidents into persistent, multi-vector attacks that exploit both human behavior and operational dependencies.

Social engineering remained the primary cause of security incidents, but the sophistication and speed of these campaigns increased dramatically. A ReliaQuest 2025 intelligence brief documented significant use of AI-generated phishing and the “ClickFix” technique, in which employees are tricked into copying malicious commands disguised as troubleshooting steps. These campaigns exploited the dispersed nature of many organizations in the transportation industry, such as remote workforces and third-party dispatch teams, to bypass centralized corporate defenses (ReliaQuest, What’s trending: Top cyber attacker techniques, June-August 2025, 2025). Bad actors regularly pose as IT help desk team members and persuade remote employees to install “support software” which is, in fact, a Remote Access Trojan (RAT). A single compromised account often provides sufficient access to dispatch platforms, billing applications, email, and load boards to enable data theft and operational disruption, or cargo-related crimes. The Cybersecurity and Infrastructure Security Agency (CISA), NMFTA, and most cybersecurity professionals continue to

provide ongoing emphasis on the criticality of workforce education as the most cost-effective control against social engineering. Recommendations included scenario-based exercises that mirror real-world workflows. For example, training programs that teach employees to verify pickup authorizations, confirm payment instructions through out-of-band channels, and validate digital identities directly correspond to reductions in fraud-related losses.

Abuse of the Server Message Block (SMB) file-sharing protocol will remain elevated in 2026 due to the widespread availability of this protocol in the target landscape (ReliaQuest, What’s trending: Top cyber attacker techniques, June-August 2025, 2025). Ransomware operators exploit these shares to access and encrypt business-critical data directly, bypassing endpoint protection tools completely. This abuse of trusted protocols highlights ongoing insufficient zero-trust adoption and exposes a persistent operational dilemma: Systems considered indispensable in daily operations, and too critical to limit, are also the ones most easily leveraged for malicious purposes.

Cyber-enabled cargo crime continued to leverage the blind spots between cybersecurity, operational security and physical security. Organized cargo crime operations increasingly combined social engineering with direct cyber intrusions to compromise cargo shipments. Attackers gained access to carrier portals, FMCSA profiles, and load boards through phishing and stolen or purchased credentials, leveraging this access to alter dispatch orders, transmit fraudulent bills of lading (BOLs), and compromise carrier identities.

The operational impact of these schemes is severe. Stolen shipments leave little identifiable paper trail, insurance claims spike, and reputational harm to carriers (particularly smaller fleets and independent owner operators) causes significant financial damage. Analysts from CargoNet and Overhaul found that social engineering and identity fraud were common denominators in nearly all large-scale thefts reported during 2025 (OverHaul 2025).

Supply chain security pressures and concentration risks continue to mount as fleets continue to increase their reliance on external software and data exchange. Multiple campaigns in 2025 exploited vulnerabilities in third-party systems like Cleo Harmony, Oracle Fusion Cloud, and Salesforce integrations used in the transportation industry (ReliaQuest, ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report, 2025). By compromising these types of intermediaries, attackers gain potential indirect access to hundreds of downstream carriers and brokers. This weaponization of trusted relationships again illustrates a systemic weakness. The transportation sector's operational interconnectivity, while improving speed and efficiency, also increases the blast radius of a single cyberattack due to elevated concentration risk across the industry.

The intersection of operational technology (OT) and information technology (IT) will continue to expose new vulnerabilities across the critical infrastructure sectors in 2026. As telematics systems, routing software, and vehicle maintenance platforms expand their integrations into cloud ecosystems, the potential risk of an attacker pivoting

from IT networks into vehicle systems grows. Additionally, with the transportation sector's heavy reliance on telematics systems, door sensors, temperature control units, cargo monitoring devices, and other similar technology, the threat landscape is extending into these essential systems as well. These risks represent serious potential threat vectors for the transportation sector and warrant diligent monitoring in order to ensure detection and response preparedness across the industry.

To manage this converged threat landscape, leading fleets are adopting segmented network architectures that isolate critical systems from general IT assets. Multi-factor authentication for all remote sessions, role-based and attribute-based access controls (RBAC, ABAC) for all systems, and continuous logging and monitoring of administrative accounts are baseline expectations rather than aspirational goals. Broader acceptance of the value of, and need for, privileged access workstations (PAWs) for administrators and strict controls limiting the use of admin accounts for non-admin functions are gaining significant traction in the industry. The most advanced carriers are deploying anomaly-detection solutions capable of recognizing behavioral deviations, such as unauthorized load cancellations or abnormal account login patterns within seconds. These adaptive measures represent a fundamental shift in mindset from static, compliance-driven cybersecurity programs toward nimble and forward-thinking whole-of-operation defenses.

Looking ahead to 2026, the operational cybersecurity landscape will continue to be dominated by three primary factors.

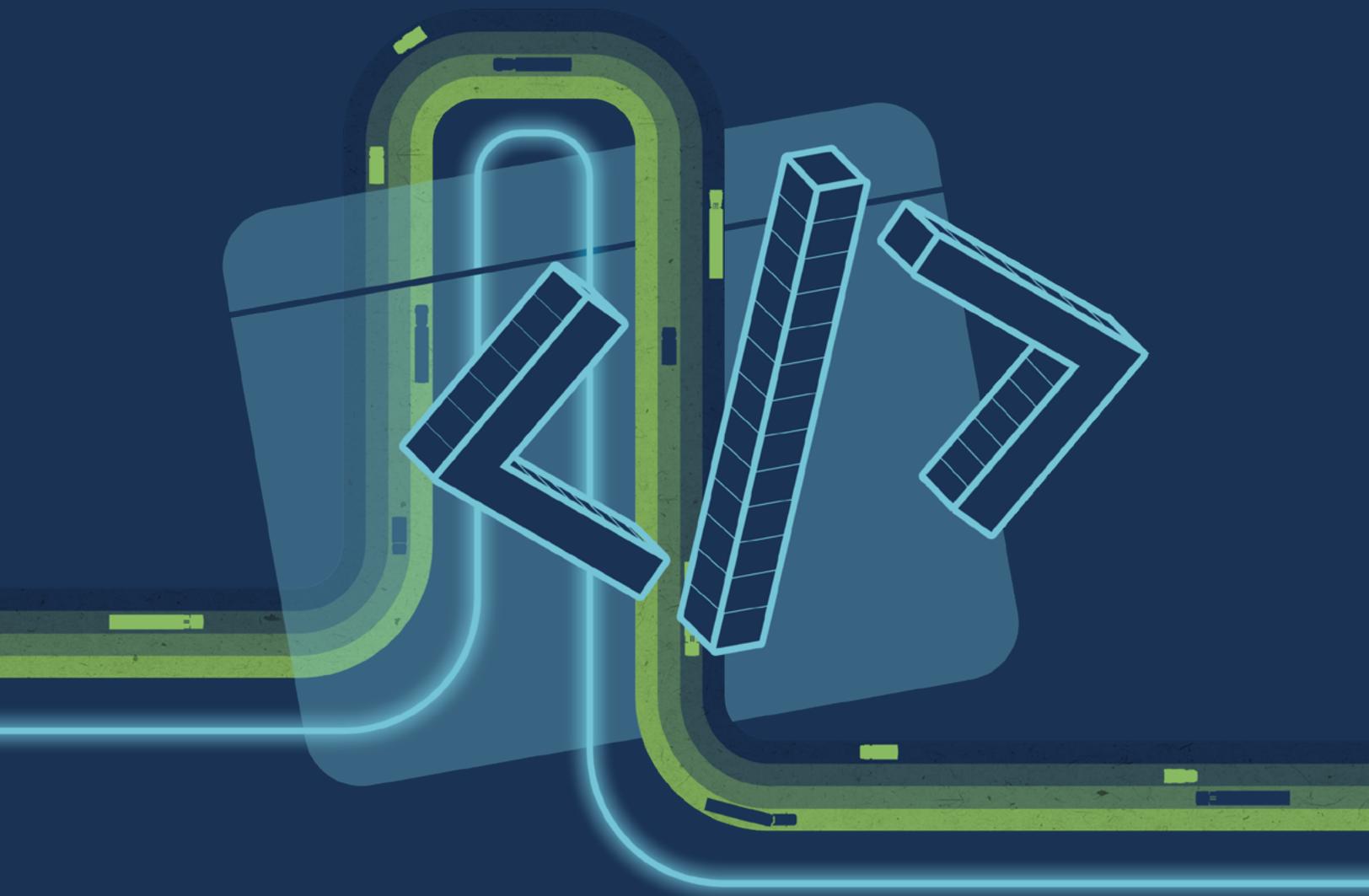
First, the persistent risk presented by the human element: Social engineering and insider compromise will remain leading risks as attackers refine AI-assisted deception to leverage weaknesses in human emotions, innate trust biases, and susceptibility to stress.

Second, the exploitation of operational trust between employees and their systems, and between partners across the transportation ecosystem, will continue to provide highly efficient and successful pathways for attackers.

Third, automation and attack speed increases will force the industry to increasingly adopt and rely on continuous monitoring and automated detection and response tooling.

For transportation companies, the operational perimeter is now everywhere: employees, data, trading partners, cargo, and the intersections between these elements. Sustaining resilience will require embedding cybersecurity into every operational process across the organization, rather than treating it as a bolt-on component or separate business function.

DIGITAL ASSET CYBERSECURITY TRENDS

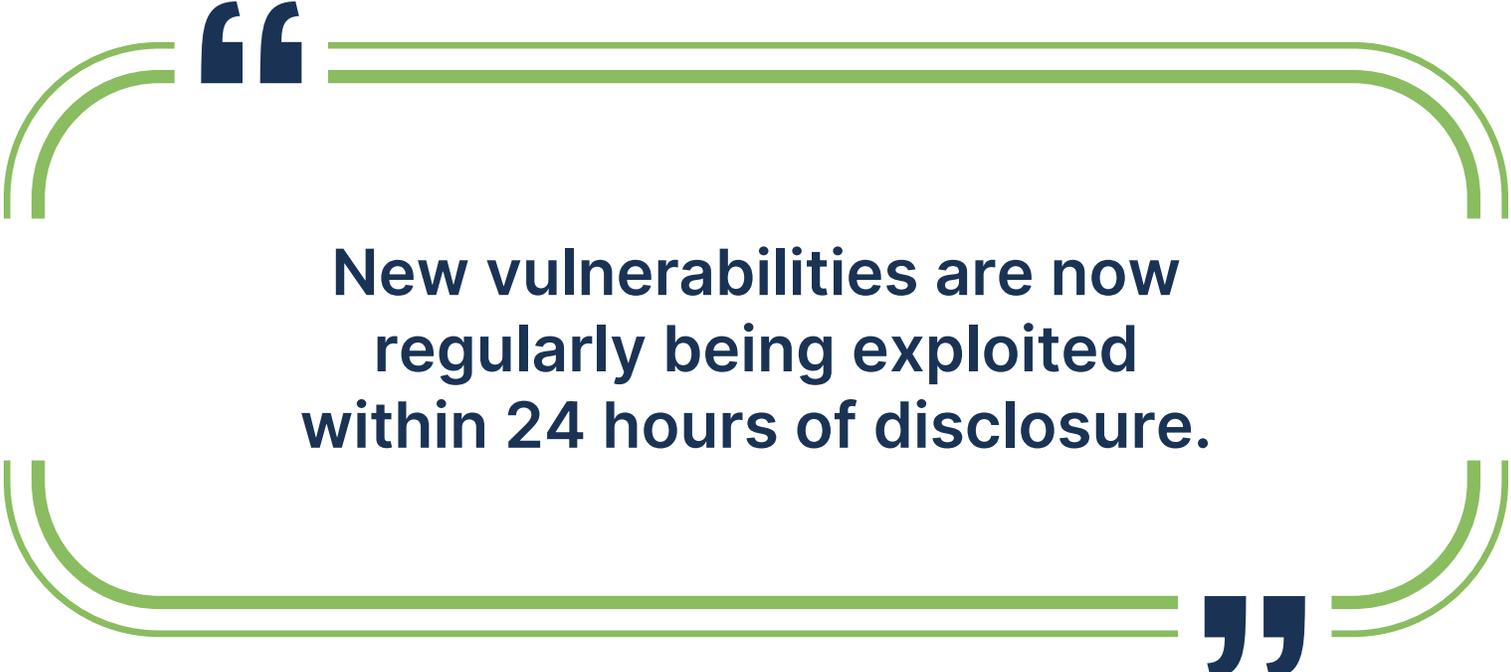


The protection of data, applications, and connected systems continue as a core cybersecurity concern. Fleets, brokers, and third-party platform providers are accelerating their migration to cloud platforms, so ransomware and data extortion groups are adapting by exploiting these same digital ecosystems that enable increased operational efficiency. The resulting environment is one where digital compromise now increasingly translates into physical and financial disruption. Data integrity is arguably overshadowing data confidentiality in some circumstances. Attackers aren't just stealing data, they are altering and fabricating digital records such as BOLs, proofs of delivery, GPS locations, and driver logs to facilitate theft and increase the pressure of extortion campaigns. As the transportation sector's administrative processes grow increasingly digital-first, ensuring both authenticity and immutability of electronic records will be a critical defensive requirement throughout 2026.

ReliaQuest and NMFTA both documented a shift in attacker strategy away from indiscriminate encryption and toward precision operations designed to maximize business impact and to increase the bad actor's leverage (ReliaQuest, ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report, 2025). Many ransomware affiliates have timed attacks around peak shipping periods (holiday seasons, end-of-quarter delivery cycles, major weather events) when downtime would cause the greatest financial pressure. These incidents highlight how trucking companies of all sizes represent a unique form of critical infrastructure, one that underpins all aspects of the U.S. economy and supply chain.

The fragmentation of major ransomware groups such as LockBit and RansomHub in mid-2025 resulted in an explosion of smaller, specialized crews. By late 2025, more than 80 active ransomware brands were recorded globally, dozens of which targeted companies in the transportation sector or vendors on which the sector depends. These groups frequently combine double-extortion tactics with data manipulation. Stolen files were often altered before being published on leak sites, magnifying reputational damage. Attackers exploited public perception of cybersecurity weakness to coerce faster payments by threatening to publicize "evidence" of poor cyber hygiene to customers and partners.

The exploitation of legitimate virtual private network (VPN) gateways and the weaponization of remote management and monitoring (RMM) tools have become central enablers of ransomware and extortion attacks. Common tools used by IT departments to manage endpoints, including AnyDesk, ScreenConnect, and standard remote desktop protocol (RDP), are being hijacked to deploy malicious scripts, escalate privileges, and execute exfiltration or encryption remotely. A significant surge in RMM-related lateral movement occurred in 2025, with several transportation sector victims compromised through authorized administrative utilities that had been weaponized by adversaries. Because these tools are vital for managing distributed environments and remote employees, simply removing them is not feasible. Instead, effective defense strategies emphasize strict access control, prevention of unauthorized installations, activity logging, and segmentation of administrative networks.



New vulnerabilities are now regularly being exploited within 24 hours of disclosure.

One of the most alarming developments in 2025 that is projected to carry over into 2026, is a sharp uptick in the number of so-called “one-day” attacks, the rapid exploitation of newly disclosed but unpatched vulnerabilities. In several incidents, exploits have been detected in the wild within 24 hours of vulnerability disclosure—well before vendors published patches and far outpacing the ability of IT teams to apply fixes. This contraction of the exploitation cycle is being driven by automated scanning and weaponization of proofs-of-concept by threat groups operating continuous reconnaissance networks enhanced with AI-enabled tools. The [CISA Known Exploited Vulnerabilities \(KEV\) catalog](#) expanded at an unprecedented rate in 2025, with numerous entries related to commonly used remote access gateways and management APIs. This acceleration of exploit development underscores how continually shrinking patching timelines have become the new reality for defenders, particularly in critical infrastructure environments operating round-the-clock systems.

Concentration risk is emerging as a defining issue in digital asset security as vendors continue to consolidate. The transportation sector relies heavily on an increasingly narrow set of software vendors and data intermediaries to manage compliance, load matching, telematics, and to facilitate payments. This reliance creates systemic vulnerabilities: A single compromise in one vendor can ripple across hundreds of additional operations at unprecedented speed, as was seen with the Cleo and Oracle breaches in 2025. This concentration risk mirrors that of other critical infrastructure sectors such as energy and finance, but with far less regulatory oversight.

Cloud environment exploitation trends also revealed a shift in attacker methodology. Instead of breaching on-prem systems, adversaries focused on targeting misconfigured APIs and insecure integrations between cloud-based systems. The Shiny-Hunters campaign exemplified this evolution. By compromising a Salesforce integration, attackers exfiltrated entire customer data-

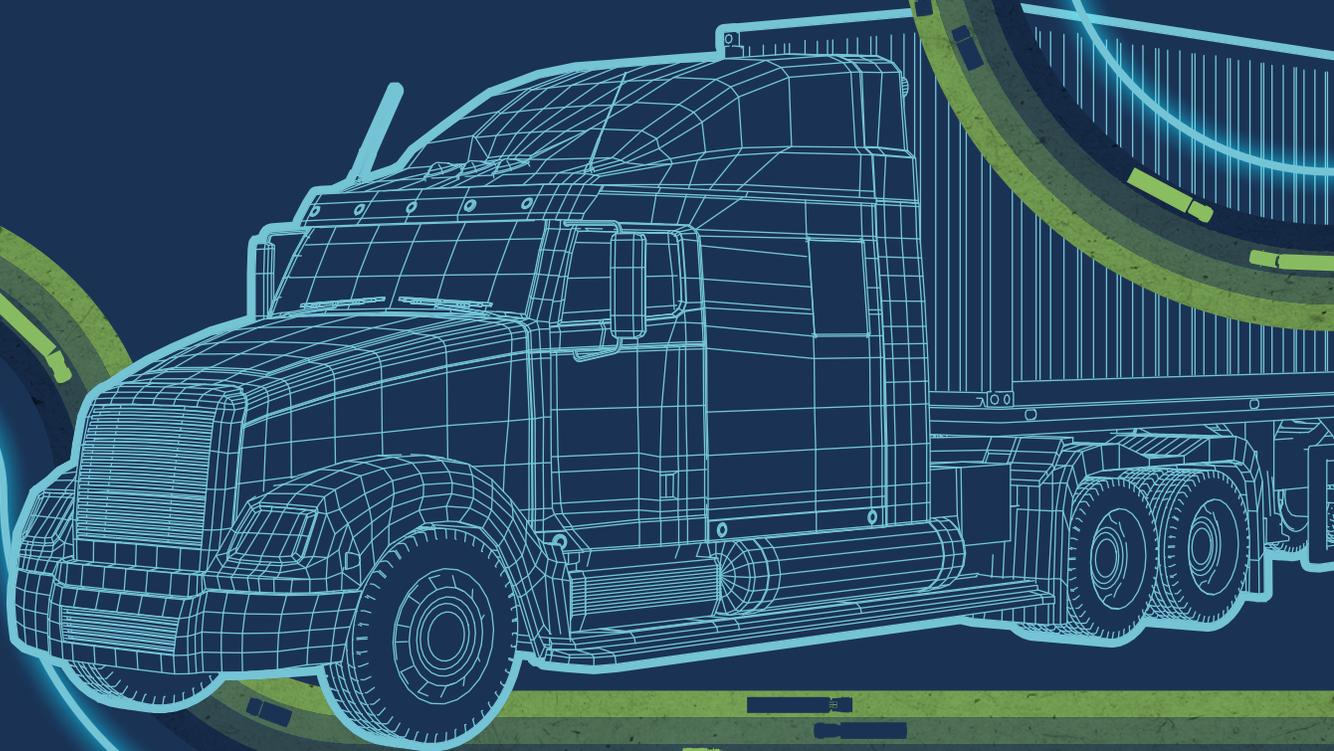
bases containing shipment records, pricing data, and account credentials. These types of intrusions easily bypass traditional defensive postures and force a rethinking of how the perimeter is defined, while also emphasizing the need for continuous configuration monitoring, strict identity and privilege controls, and comprehensive vendor risk management.

Increasingly, bad actors remain undetected by either delaying or altogether forgoing the deployment of ransomware to encrypt data, preferring instead to exfiltrate data at scale and use the threat of release of that data to extort a ransom payment from victims. The combination of these evolving threats has forced organizations in the transportation industry to redefine their cybersecurity priorities. Preventing intrusion is not sufficient. Resilience now depends on visibility, segmentation, detection of data exfiltration, and recovery capabilities. Industry best practices such as prioritizing the adoption of zero-trust architecture, immutable backup solutions, and continuous monitoring remain, but now should be incorporated into security programs with increased urgency. [The NMFTA's Cybersecurity Best Practices Guidebooks](#) recommend specific safeguards and are recommended for further reading on specific actions that fleets can take to prepare their operations for the continued evolution of these threat trends.

Looking ahead into 2026, transportation sector cybersecurity leaders anticipate continued escalation of the threats mentioned above. Ransomware groups are expected to expand their use of automation and AI-driven reconnaissance to identify high-value operational data, while defenders will increasingly

turn to threat intelligence sharing and predictive analytics to anticipate exploit trends. Concentration risk will remain a structural challenge until the sector diversifies its technology providers or mandates standardized security controls across platforms utilized in the industry. The most resilient fleets will be those that treat digital asset protection as mission-critical and integrate cybersecurity across the business, including safety, maintenance, operations, and business continuity planning.

PHYSICAL ASSET CYBERSECURITY TRENDS



Physical assets remain at the heart of the transportation sector, and present challenges that traditional cybersecurity frameworks weren't designed to address. While enterprise systems and infrastructure have, understandably, been the focus of cybersecurity efforts, heavy-duty trucks and trailers themselves still play a vital role in the broader security picture. As they remain a potential attack surface, these assets need to be considered in a holistic cybersecurity defense posture to minimize possible risk. Several physical asset cybersecurity trends emerged in 2025 that are expected to persist and intensify in 2026.

The sharp rise in cargo crime that was observed in 2025 was accompanied by a noticeable increase in the sophistication of coordinated theft operations. A prevalent technique used was GPS spoofing, where criminals manipulate location data of trucks or trailers to conceal unauthorized route changes or to mislead tracking systems during load thefts. These attacks are often used in conjunction with social engineering techniques—such as phishing—to exploit call centers, dispatch operations, or other staff involved with shipment verification and communication. Looking ahead, cargo crime is expected to continue rising in 2026 as criminal groups become more organized, employ increasingly advanced techniques, and view the transportation sector as an ever more profitable target (Verisk, 2025).

The growing complexity of these threats is also reflected in the technology embedded within the trucks themselves. Telematics devices as a threat vector is another theme that continued through 2025. Adoption continues to accelerate as fleets rely on connected

systems to boost efficiency, safety, and productivity, but security practices around and within these devices continue to lag. While telematics have become indispensable to modern fleet operations, their remote connectivity introduces new opportunities for wireless attacks targeting tractors and trailers. Compromised telematics units could potentially serve as a bridge into broader enterprise systems, particularly when weak API security or unsecure cloud integrations are present. There is additional risk with the use of aftermarket or poorly maintained devices that often lack basic safeguards. Now, more than ever, it is essential to audit any equipment installed into trucks, and to push original equipment manufacturers (OEMs) and suppliers to embed security by design into their products to minimize introduction of unnecessary risks into critical assets.

Nation-state actors continued to probe and, in some cases, gain access to our nation's critical infrastructure, as evidenced by the actions of groups such as Salt Typhoon and Volt Typhoon. While there are limited instances of the transportation sector being targeted directly, the sector is critical infrastructure, with trucking specifically forming the backbone of the national supply chain. Supply chain attacks, where component suppliers are compromised and bad actors gain long-term access to vehicle systems, have emerged as a key risk.

As more component parts are sourced from regions with lower manufacturing costs, such as the People's Republic of China (PRC), concerns around country-of-origin arise, including the possibility of backdoors or other hidden exploits being built into parts.

In 2025, these concerns led to the introduction of regulations aimed at mitigating the use of components manufactured in certain high-risk regions for connected vehicles. Although this rule currently only applies to passenger vehicles, issues surrounding country-of-origin risk and the measures designed to address them are expected to remain a regulatory focus into 2026.

Overall, 2025 saw a steady increase in interest in heavy-duty vehicle cybersecurity efforts and research. While no attacks specifically on trucks in the wild have been publicly released, there are ongoing trends that highlight the need for continual strengthening of these systems and surrounding environments.

“

**High-fidelity deepfakes and
AI-generated content are
redefining social engineering.**

”

EMERGING TECHNOLOGY CYBERSECURITY TRENDS



By the end of 2025, the transportation sector was both benefiting from and being reshaped by emerging technologies that redefine the speed, precision, and complexity of cyber-threats. Artificial intelligence, automation, and the integration of smart systems across the transportation ecosystem are simultaneously enabling improved efficiencies and creating new attack vectors for cybercriminals. The challenge for the transportation sector in 2026 is clear: We must harness these innovations without becoming their victim.

Machine learning (ML) and artificial intelligence now stands at the center of both offensive and defensive cybersecurity strategies. From a threat perspective, AI has democratized deception. ReliaQuest's 2025 report detailed how generative AI models are being leveraged by attackers to create contextually accurate phishing emails, spoofed BOLs and invoices, and even dispatch-related messages tailored specifically to a target organization (ReliaQuest, ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report, 2025). Gone are the grammatical errors and inconsistent formatting that once served as clear red-flags. Instead, modern phishing lures include accurate shipping references, legitimate logos, and personalized content crafted from scraped online data. These highly believable phishing campaigns have driven a significant increase in social engineering success rates across the transportation sector.

Voice and video deepfakes and smishing (SMS-based phishing) attacks are beginning to expand this threat further. Fraud investigators and insurers documented multiple cases in 2025 where criminals used

AI-generated voice calls to impersonate managers or company executives. These new attack methods rely not on hacking systems, but on manipulating trust, and leveraging the speed at which the transportation sector operates. As deepfake and synthetic identity crimes rise, lawmakers and regulators are beginning to explore disclosure and accountability requirements for AI-generated content (California, 2025).

With the widespread adoption of AI related tools into operational workflows of many organizations, the risk of proprietary data exposure is elevated. 2026 will see this trend continue, potentially increasing further, as security awareness and methodologies surrounding secure AI use lag behind the rate at which organizations pursue efficiency gains to keep pace with a changing competitive landscape. Agentic AI and internal AI-powered workflows are commonly being rolled out with a false sense of security and an underestimation of the data privacy risks that they introduce. Machine identities and the rights granted to agentic deployments are inadequately managed as the security learning curve around this rapidly expanding technology continues to steepen.

AI is also being used for large-scale reconnaissance. Automated scanners powered by ML algorithms now sweep the internet continuously for exposed APIs, misconfigured cloud storage buckets, or unpatched systems. These tools can identify vulnerabilities across thousands of potential victims in minutes. For adversaries, this automation enables mass exploitation campaigns that require little manual effort. AI-driven reconnaissance, followed by

fully automated exploitation and lateral movement, has the capability of compressing the entire breach lifecycle, and therefore the available response time, to well under an hour.

The same technology is also transforming defensive operations. AI-based behavioral analytics systems are becoming indispensable for detecting subtle anomalies in logins, data access or movement, and even vehicle telemetry. Organizations deploying properly configured AI-assisted monitoring solutions achieve significant reductions in detection times and experience far earlier notifications of intrusions than human analysts alone could provide. Machine learning models trained on operational baselines are able to flag deviations such as unusual route alterations, abnormal file access, or off-hours account use in near real time. These tools are proving particularly valuable in 24-hour industries like transportation where manual oversight simply cannot keep pace with the volume of digital activity.

The competition between automated offense and automated defense is quickly defining a new cybersecurity balance point. Both attackers and defenders are leveraging ML and other forms of AI to accelerate both decision-making and action. While attackers are often thought to have the advantage of simplicity on their side (the well-known “they only need to find one successful path”), defenders can effectively gain the upper hand with a single real-time detection and a well-configured defense. Catching the bad actor at any phase of the attack chain forces them to change tactics, invest more time and resources, and often start their entire campaign over. This reality drives home the importance of layered security architectures capable of recognizing subtle behavioral

signals that pure rule-based legacy systems might miss.

As emerging technologies evolve, cybercrime operations continue to adapt in parallel. Automations increasingly allow smaller and less skilled criminal groups to deploy complex multi-stage intrusions that once required significant technical expertise. The diversification of targets has continued throughout 2025, with the number of indiscriminate automated attacks surpassing refined, targeted operations. Fewer fleets now subscribe to the misconception that they are “too small” or “too niche” to attract attention from major cybercrime operations, and the past year has confirmed that every operation in the sector is now a viable target for autonomous, AI-assisted campaigns that can identify and exploit weaknesses at unprecedented scale and with unprecedented speed.

Defensively, the industry’s adoption of AI is beginning to mature beyond the realm of chatbots and AI-powered spam detection. AI-driven intrusion detection, autonomous defensive tools, and predictive analytics are moving from theoretical studies and pilot programs into operational use. However, these technologies remain only as effective as the data feeding them. Poor data hygiene, limited visibility into third-party tools and processes, and a lack of interoperability between systems continue to provide headwinds against the development of fully automated defense. Poorly configured, or inadequately tested AI deployments continue to create additional threats for the industry as the race to adopt these newer technologies is impacted by the pressurized demands of speed and efficiency in the transportation sector.

Emerging technology often proves to be a double-edged sword. Artificial intelligence, automation, and IoT innovations promise greater safety, speed, accuracy, and efficiency. These same technologies also empower adversaries to attack faster, deceive more convincingly, and scale beyond human capabilities and limitations. The organizations that continue to thrive in this new environment will be those that treat AI not as a replacement for human expertise, but as a force multiplier across both business operations and cybersecurity. These new technologies must be integrated with well-designed and disciplined governance, continuous training, and deliberate strategy.

PRIVACY LAWS, REGULATORY LANDSCAPE, GEOPOLITICAL INFLUENCES AND IMPACTS



The balance between security and privacy will become increasingly complex in 2026 as fleets adopt more advanced driver monitoring and telematics systems capable of recording troves of sensitive operational data. Carriers will need to navigate data privacy rules governing the use of driver biometrics, camera footage, and behavioral analytics.

Beyond these issues surrounding data privacy and the use of AI, the regulatory environment for cybersecurity in the transportation sector will evolve rapidly in 2026. These changes reflect the growing recognition that cyber threats pose systemic risks to national supply chains. Government, insurers, and industry associations are increasingly treating cybersecurity not as an IT compliance function, but as a prerequisite for operational reliability. As a result, the transportation sector will enter 2026 facing a complex mix of new mandates, privacy obligations, and voluntary frameworks designed to improve resilience and protect sensitive data. These changes will increase pressure on vendors supporting the transportation sector due to heightened focus on proactive vendor management practices.

At the federal level, multiple agencies advanced cybersecurity rulemaking with direct implications for the transportation sector broadly, and the trucking industry specifically. The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) both prioritized the transportation systems sector within their broader critical infrastructure protection strategy. The forthcoming Cyber Incident Reporting for Critical Infrastructure

Act (CIRCI) regulations (expected to take effect in Q2 2026), will require certain transportation and logistics entities to report any significant cybersecurity incidents within 72 hours of discovery (Cyber Incident Reporting for Critical Infrastructure Act (CIRCI) Reporting Requirements, 2024). This requirement is not dissimilar to the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) requirements already applicable to publicly traded entities, although CIRCI requirements differ on specific, technical qualifiers and reporting timelines. The message is clear: Cybersecurity breaches represent an undeniable risk beyond the victim organization itself. This new requirement will represent a major shift for many privately owned trucking companies and brokerage operations that have historically lacked formalized incident reporting requirements. Preparations for 2026 and the anticipated enactment of CIRCI will include proactively aligning incident reporting workflows with [CISA's draft guidance and incident reporting system](#).

On the policy front, the National Cyber Director indicated in October 2025 that updates to the White House's National Cybersecurity Strategy Implementation Plan (NCSIP) would involve a focus on collaborative partnerships between government and industry as well as the expectation that private sector should have to meet minimum standards for cybersecurity. Executive branch directives issued throughout 2025 encouraged the adoption of "secure by design" principles in critical industry software, applicable to transportation sector software and systems. These directives align with CISA's Secure by Design Framework (Cybersecurity and

Infrastructure Security Agency et al, 2023), which outlines baseline security expectations for vendors providing services to critical sectors. Vendors that handle operational data or provide software or systems to the transportation sector will experience increased expectations to demonstrate alignment with these guidelines in 2026.

Privacy and data protection obligations also expanded at the state level in 2025. California, Virginia, Colorado, and several other states have enacted or strengthened consumer data privacy laws with provisions covering employee or contractor data. For carriers operating interstate fleets, this means driver information (telematics logs, video footage, and biometric identifiers such as those captured by in-cab safety systems) increasingly falls under a patchwork of overlapping privacy regulations. The California Privacy Rights Act (CPRA) and its various counterparts in other states mandate that companies provide clear notice of data collection, and many require that companies allow employees to access or request deletion of their personal data. Ongoing compliance with these regulations in 2026 will require fleets to implement data governance programs that track what operational data covered under these privacy regulations is collected, how it is classified or identified, where it is stored, and how it is shared with third parties.

The insurance market continues to reinforce these regulatory shifts through contractual obligations. Underwriters are increasingly requiring concrete evidence of cybersecurity maturity as a condition of policy renewal or claims eligibility. Insurers now commonly request proof of MFA, endpoint protections,

encrypted backups, incident response planning, and data governance. These private-sector pressures, while not statutory, effectively function as regulating mechanisms by incentivizing stronger controls and improve cyber hygiene across the industry. Fleets that fail to demonstrate compliance will continue to face higher premiums or exclusions for cyber-related losses in 2026.

Government and regulatory emphasis on supply-chain resilience is evolving beyond compliance requirements to active collaboration. In 2025, CISA, TSA, and other federal agencies expanded their collaborative efforts with industry stakeholders. NMFTA, as a participating partner, continued to play a central role in shaping these efforts by bridging public-private communication between fleets, law enforcement, and federal cyber defense teams. These partnerships will continue to gain momentum in 2026, and they represent a shift from reactive enforcement toward proactive collaborations and threat intelligence integration into the transportation sector.

CIRCI will likely come into force in March of 2026 and if so, will introduce structured reporting and accountability. The U.S. Department of Transportation's (USDOT) increased focus on the cyber-enabled cargo crime epidemic is highly likely to result in an elevated focus on cybersecurity within the transportation sector at various levels of government. The growing number of state-level privacy laws will compel carriers to treat driver records and telematics data as protected personal information, requiring enhanced consent management and data governance policies. AI safety regulations,

at the state level particularly, will remain a fast-moving and dynamic force in the regulatory landscape. Meanwhile, insurers and investors will continue to reward measurable cyber maturity, effectively turning resilience into a competitive advantage.

The transportation sector appears to be on track to experience the convergence of cybersecurity governance and privacy compliance. Carriers that adopt a unified approach that includes technical controls, strong data management, and cross-jurisdictional policy awareness will not only meet regulatory expectations but will also contribute to increased trust throughout the transportation sector.

CONCLUSION

The year ahead will present unprecedented challenges in the cybersecurity landscape for the transportation sector. Cyber-enabled cargo crime will remain a growing threat; sophisticated cybercriminals will continue to mount ever-more complex attacks with increasing speed and precision. AI, the great double-edged sword of technological advancement, will bring new security challenges and will up the ante in the constant game of cat-and-mouse between bad actors' intent on disruption, fraud, and data theft and the defenders tasked with protecting organizations in the crosshairs.

However, the transportation sector has demonstrated already that it is rising to the challenge. Collaboration across the sector is at an all-time high, with cybersecurity professionals, executives, law enforcement, government agencies, and operations teams sharing threat intelligence, indicators of compromise, and lessons learned with greater transparency than ever before.

The impact of cyber-enabled cargo crime has been felt by stakeholders across the industry, and the private sector, the public sector, and non-profit organizations and associations alike have said: "Enough!" Through consistent and concentrated collaboration, the tide will turn against the bad actors who target the transportation sector looking for easy profits. Constant tailored awareness training, organized intelligence collections and dissemination, coordinated research and security-first development and integrations are moving the needle.

Incorporating cybersecurity, operational security, and physical security as three parts of an integrated whole into the cultural fabric of every organization across the sector will reduce the risks faced by all. Together, the members of the transportation sector regularly do the impossible. Through collaboration, consistent focus on strategic solutions, and good old fashioned hard work, securing the sector against cyber-enabled cargo crime, extortion and disruptions will be one more in a long line of success stories that this industry will be able to proudly share.

NMFTA CYBERSECURITY RESOURCES

NMFTA Cybersecurity Best Practices Guidebooks

[Strengthen Your Fleet's Cyber Resilience >](#)

Vendor Risk Assessment Framework

[Evaluate, onboard, and monitor third-party vendors with confidence >](#)

NMFTA Cargo Crime Reduction Framework

[Fight Back Against Cyber-Enabled Cargo Theft >](#)

NMFTA Cybersecurity Webinar Series

[Empower Your Workforce. Stay Ahead of Emerging Threats >](#)

Annual NMFTA Cybersecurity Conference

[Where the Transportation Industry Unites to Defend the Supply Chain >](#)

ABOUT US

NMFTA Cybersecurity is a division of the National Motor Freight Traffic Association, Inc. (NMFTA)[™], non-profit organization. NMFTA Cybersecurity's mission is to promote, advance, and improve the welfare and interests of the motor carrier industry. We do this through research, education, lobbying and developing industry standards and best practices. Our goal is to have the most informed membership who not only grow profitable, but efficiently run operations and protect against new challenges resulting from the digital era.

Learn more at nmfta.org/cybersecurity

Follow Us:



APPENDIX

Industry, Cybersecurity & Technical Acronyms

- **ABAC** – Attribute-Based Access Control
- **AI** – Artificial Intelligence
- **API** – Application Programming Interface
- **BEC** – Business Email Compromise
- **C2** – Command and Control
- **EDR** – Endpoint Detection and Response
- **EPP** – Endpoint Protection Platform
- **GPS** – Global Positioning System
- **IoC** – Indicator of Compromise
- **IoT** – Internet of Things
- **IT** – Information Technology
- **KEV** – Known Exploited Vulnerabilities
- **MFA** – Multi-Factor Authentication
- **OT** – Operational Technology
- **PAW** – Privileged Access Workstation
- **POD** – Proof of Delivery
- **RaaS** – Ransomware-as-a-Service
- **RAT** – Remote Access Trojan
- **RBAC** – Role-Based Access Control
- **RDP** – Remote Desktop Protocol
- **RMM** – Remote Monitoring & Management
- **SaaS** – Software-as-a-Service
- **SMB** – Server Message Block
- **TTP** – Tactics, Techniques, and Procedures
- **VPN** – Virtual Private Network

Transportation & Regulatory Acronyms

- **BOL** – Bill of Lading
- **CISA** – Cybersecurity and Infrastructure Security Agency
- **CIRCA** – Cyber Incident Reporting for Critical Infrastructure Act
- **CPRA** – California Privacy Rights Act
- **DHS** – Department of Homeland Security
- **DOT** – Department of Transportation
- **ELD** – Electronic Logging Device
- **FMCSA** – Federal Motor Carrier Safety Administration
- **FTC** – Federal Trade Commission
- **NCSIP** – National Cybersecurity Strategy Implementation Plan
- **OEM** – Original Equipment Manufacturer
- **PRC** – People’s Republic of China
- **SEC** – Securities Exchange Commission
- **TMS** – Transportation Management System
- **TSA** – Transportation Security Administration

References

California. (2025, October 13). AB-853 California AI Transparency Act. California. Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB853

Cybersecurity and Infrastructure Security Agency et al. (2023, October 25). Secure by Design. Retrieved from https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) reporting requirements. (2024, April 4). Federal Register. <https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements>

ReliaQuest. (2025, October 24). ReliaQuest 2025 Trucking Trends NMFTA Internal Intelligence Report

ReliaQuest. (2025, September 23). What's trending: Top cyber attacker techniques, June-August 2025. Retrieved from <https://reliaquest.com/blog/threat-spotlight-top-cyber-attacker-techniques-june-august-2025>

Verisk. (2025, October 31). Cargo Theft Holds Steady in Q3, Organized Crime Drives Surge in High-Value Cargo Theft Across U.S. and Canada. Retrieved from <https://www.verisk.com/company/newsroom/cargo-theft-holds-steady-in-q3organized-crime-drives-surge-in-high-value-cargo-theft-across-u.s.-and-canada/>



© Copyright 2025, National Motor Freight Traffic Association, Inc. (NMFTA)™ All rights reserved.

1001 N Fairfax St, Ste 600, Alexandria, VA 22314-1798