Cybersecurity in Transportation: A Look at Recent Cyber Attacks & What They've Taught Us

As businesses have raced to adopt web-based systems to streamline operations and drive efficiencies across their operations, the threat of cybercrime has loomed large. For industries like trucking and logistics, leveraging online tools, IoT, and Big Data is no longer a matter of gaining a competitive edge; these modern solutions have become essential to doing business in the 21st century. But unfortunately, these efficiency gains also present vulnerabilities.

No matter the size or scope of your business, cybercriminals have their sights set on your data repositories, which can be exploited to their immense gain. In the past decade, we've seen that no company is safe. While transportation, trucking, and logistics companies may experience attacks less frequently than those in other sectors, including healthcare and finance, all that could change. In fact, recent trends reveal that cyberattacks against IoT devices has risen by 400%.[i] This steady uptick paints a grim picture, but it begs the question: Can cyberattacks be prevented?

The answer is yes — but only with the right approach.

In this guide, we'll discuss the best ways to strengthen your cybersecurity posture to prevent attacks like ransomware and other types of cybercrime, as well as their disastrous consequences. But first, we'll look at some recent events to provide context about the risks and vulnerabilities of the trucking industry.

Keep in mind that while these stories are unsettling, the goal here isn't to induce panic, but rather, to prompt you into planning mode so your company doesn't become another victim.

Why is transportation so vulnerable to cyberattacks?

Virtually every sector is susceptible to cybercrime, but for transportation, trucking, and logistics companies, there are unique risk factors. For one, the industry's increasing reliance on technology makes it an attractive target for bad actors. Various transportation networks have been integrated, including vehicle management, traffic control, and logistics. While these approaches have increased efficiency across the industry, it also increases risk.

Cybercriminals have a keen ability to exploit vulnerabilities in a single network that can open up access to others, allowing their malicious activities to take hold across broader operations. A multi-network breach can therefore suspend operations across multiple facets of logistics and transportation.

With an increasing reliance on digital systems, the transportation sector has near-countless opportunities for cybercriminals to carry out attacks. Leveraging digital systems for everything from route optimization to driver data means there are more vulnerabilities than ever. And IoT devices introduce an entirely different set of risks: without sufficient security measures in place for connected devices, they can easily be compromised, granting attackers access to sensitive data.

Unfortunately, trucking and logistics companies have historically been slower to adopt the appropriate cybersecurity protocols. Many businesses lack the proper leadership support, and many also fail to implement company-wide cybersecurity awareness. Startlingly, some businesses lack cybersecurity and cyber insurance altogether, making them easy targets for even novice cybercriminals.

Aside from its vulnerabilities, there are additional factors specific to trucking that make the industry such an attractive target to cybercriminals. For one, trucks across the US transport at least $82B of freight each year.[ii] Hackers know many freight and logistics companies have high-value assets at their disposal, and they'll do everything in their power to tap into them. From holding customer or company data hostage via ransomware attacks to uncovering details about our nation's most sensitive cargo, there are plenty of ways for cybercriminals to carry out attacks with disastrous implications.

Many trucking and logistics companies also have several API security concerns. Old, deprecated APIs are all too easy for hackers to break into, making it simple to orchestrate a denial of service attack that could overwhelm a website, network, or server. Even accidental data leakages are a concern; practices like poor password management pose a serious threat for companies of any size.

Technology is also becoming more sophisticated, so cybercriminals are able to get their hands on ever-evolving tools. Phishing attacks have become increasingly difficult to detect, and AI-powered tools have made impersonators extremely effective in their deception tactics.

Unfortunately, several major transportation companies have already witnessed these trends firsthand.

8 recent cyber-attacks in transportation

Cyber-attacks have unfortunately become so commonplace that it's easy to forget even the largest data breaches that have occurred within the last decade. Trucking and logistics have had a few standout instances of cybercrime. Whether it's your first time hearing about some of these or you've been following the news closely, these events and their implications can serve as a learning experience for everyone across the industry.

Here's a chronicle of the most noteworthy cyber security events in trucking and transportation.

2023

Estes Express Lines

In the fall of 2023, freight shipping giant Estes Express Lines experienced a ransomware attack which compromised the personal data of more than 21,000 people. Names and social security numbers were among the personally identifiable information (PII) exposed. Ransomware gang LockBit took responsibility for the attack.

Responses to the cyber event have been mixed: affected individuals weren't notified of the data breach until December — many weeks after the event initially took place in late September. Experts have criticized the company's delay in raising awareness, though victims were given free ID monitoring service for 12 months. Others have hailed Estes for their swift response. Upon the initial detection of suspicious activity, the entire network was promptly disconnected to prevent further spread. GuidePoint was engaged within 90 minutes, communications were restored to an operational level within five days, and customer systems were back online within a week. Estes has also stated that they'll be moving away from legacy APIs to more standardized operations.

Bottom line: Estes' quick response mitigated the damage of this cyber-attack, and their willingness to share insights with the industry and learn from the event demonstrates a commitment to future preparedness and solidarity with their peers.

Orbcomm

Another event of fall 2023, trucking and fleet management solutions provider Orbcomm sustained a ransomware attack that led to service outages. The outage prevented Orbcomm users, including some of the country's largest freight transportation companies, from using their tool to log hours and manage their fleets. The US Federal Motor Carrier Safety Administration issued a waiver allowing drivers to use paper logs until the affected devices were restored. Drivers had to rely on other communication methods, including texts, phone calls, and emails during the outage.

2020

Forward Air

In December 2020, trucking and freight logistics company Forward Air was hit by a ransomware attack orchestrated by the cybercrime gang Hades. While the company quickly engaged third-party experts, they had to take their systems offline to prevent the attack's spread, resulting in business disruptions and service delays for many of their customers. And while the company survived the attack, it cost them about $7.5M, which they attributed mainly to the suspension of electronic data interfaces with customers.[iii]

Central Freight Lines

2020 was a busy year for cybercriminals, with many taking advantage of the fact that businesses were already facing supply chain challenges and other pandemic-related strains. Less-than-truckload carrier Central Freight Lines (CFL) was a victim of a cyberattack in December 2020 which caused outages for their call center and operating systems. Like other trucking company victims, they also engaged third-

party professionals. Their systems were restored in less than a week, and none of their private data leaked to the dark web. Yet, the 95-year-old company had already been facing financial woes. The cyberattack undoubtedly contributed to their downfall, and CFL shuttered their operations less than a year later.

CMA CGM

Another 2020 event, the malware attack on CMA CGM resulted in a release of the company's private data. External access to their applications was interrupted to prevent the malware from spreading after the attack initially affected its peripheral services. Less than a year later, the company suffered a data breach that exposed the personal details of their customers.

2019 and Earlier

A Duie Pyle

In 2019, hackers disrupted the communication network of A. Duie Pyle, a transportation and logistics provider for the Northeast. The ransomware attack shut down the company's website and disrupted their ability to interface with shippers.

COSCO

In 2018, COSCO Shipping Lines, headquartered in Shanghai, sustained a cyber-attack that affected its internet connection in the US. The company took swift efforts to control the attack's impact and isolate internal networks. Service was mostly restored within several days.

Maersk

In 2017, Danish shipping company Maersk experienced a disastrous cyberattack that affect its port, deport, and terminal operations. The event is estimated to have cost the company $300M.[iv] To this day, it's considered the most devastating cyberattack in history, an incident that left the company unable to process shipping orders, freezing revenue for weeks.

A Tale of 3 Trucking Companies

As leaders in cybersecurity, we've seen the implications of ransomware and other cyber-attacks firsthand. Here's an insider's look at how three trucking companies fared following cyber events.

Transportation company #1

In late 2020, a well-known local trucking company found itself in the grip of a massive ransomware attack that knocked its operating systems and call center offline. It was 9:00 pm when we got the first call and were officially engaged post-incident to lead the recovery effort.

During an initial meeting the next day with internal IT and executive staff, we learned the full extent of the attack included over 800 computers and more than 50 servers across 75 terminals. Unfortunately, the client had minimal backups, and a significant portion of their core infrastructure was entirely encrypted, leaving them with no viable restore options. Faced with this dire situation, the company made the difficult decision to pay a $300,000 ransom.

During this time, a third-party forensics company was engaged to conduct a thorough investigation, while IT ArchiTeks worked to restore the foundational systems. In less than a week, we successfully brought most of the core operational systems back online, with the remaining systems gradually recovering over the following weeks.

Sadly, statistics show the vulnerability of SMBs, with 60% failing to recover after a cyber event. Compounded by several factors, including the cyber-attack, this century-old company shut down not long afterwards.

Transportation company #2

During a busy convention recently, an executive from a trucking company recounted with detail the ransom experience he'd endured several months prior.

With his head hung down, he admitted that though they had some security measures in place, they didn't have enough to fend off the attack. Desperate and not knowing what else to do, they opted to pay the ransom, hoping to retrieve their data and salvage the company. Unfortunately, even after the payment, they grappled with encrypted files and struggled for over a year to regain their pre-attack operations.

IT ArchiTeks entered the scene amidst their recovery efforts, tasked with conducting a cybersecurity risk assessment. Uncovering additional vulnerabilities and security gaps, our analysis empowered the company to prioritize critical security issues. Armed with a solid plan of action, they are taking steps to regain control of their environment and have begun to rebuild their systems and preserve their upstanding industry reputation.

Transportation company #3

During early 2023, we conducted a thorough cybersecurity risk assessment on an existing customer and recommended an upgrade to our comprehensive cybersecurity solution. In July, the company agreed. Over the next few months, we implemented the best tools and services in the market.

Just before the holiday season in December, the company was hit with an attempted ransomware attack from Russia. Fortunately, our cybersecurity incidence response plan worked exactly as intended. The security operations center immediately detected a cyber threat and notified the appropriate staff members. We then isolated those systems and engaged a forensics team which conducted a thorough investigation.

The forensics analysis took five days. Once the forensics team greenlit the restoration process, we had the company back up and running within 18 hours. Thanks to a carefully crafted backup data recovery plan, data was restored to within 15 minutes of the initial attack - with no data loss or encryption.

Taking a Defensive Approach to Cybersecurity

As we've seen with the examples above, the unfortunate reality is that it's not a matter of *if* a cyberattack attempt should happen to your company, but *when*. And when that day comes, the objective is to be back up and running as soon as possible, with no data lost and no major derailment of your operations.

With the right defenses in place, an attempted cybersecurity compromise can be just a minor blip. But as illustrated above, lacking the proper backups and cybersecurity tools leaves your company vulnerable to devastating consequences.

Each company has a unique risk profile, and therefore requires a tailored cybersecurity plan with robust measures in place. Only cybersecurity experts can perform a comprehensive risk analysis to identify gaps and present solutions to address vulnerabilities. Most transportation companies can benefit from at least some upgrades, especially since as technology evolves, cybercriminals are likewise becoming more sophisticated in their strategies. But our team knows how to help you stay one step ahead, empowering you to take a proactive instead of reactive approach to cybersecurity.

Getting Started with Cybersecurity: Tips for Transportation Companies

While effective cybersecurity calls for a business-specific approach, there are several best practices you can begin implementing now. Our experts can help you get up to speed, but here are a few basic principles to bear in mind.

- Ensure you have a top tier managed detection and response (MDR) and end point detection and response (EDR) on every device/server throughout your organization.
- Implement a Zero-Trust solution to contain and minimize the impact of breaches and ransomware enterprise wide.
- Make that you have sufficient backup systems in place. As illustrated in the story of Transportation Company #1, having minimal backups can leave you with little to no restoration options following a cyberattack.
- Ensure technical measures receive the proper attention. IT teams or third-party experts should focus on anti-malware software, network segmentation, and patching.
- Have your cybersecurity infrastructure thoroughly audited to test systems and identify vulnerabilities.
- Establish a comprehensive incident response plan, and be sure to consult with legal teams.

- Train employees on how to spot phishing attacks and other threats. Perform refresher courses and introduce new training sessions as new threats evolve.
- Focus specifically on API security, as old APIs (also known as “zombie” APIs) pose especially large threats. Use API keys, store data fully encrypted on servers, and use two or more factors for hashing and encryption.
- Invest in the right amount of cyber insurance to safeguard your financial assets against the economic effects of a data breach or other losses related to cybercrime.

If all of this sounds overwhelming or you’re still unsure where to start, allow our team to help. IT ArchiTeks is made up of cybersecurity experts who can provide tailored solutions to safeguard your company and its assets against cyber-attacks. Enlist our professional team to handle all of your trucking or logistic company’s cybersecurity needs so you can continue to focus on core business initiatives. Contact us now for an assessment.

---

[i] https://www.iotevolutionworld.com/iot/articles/457529-better-security-required-iot-malware-attacks-hit-400.htm

[ii] https://www.bts.gov/newsroom/north-american-transborder-freight-41-november-2023-november-2022

[iii] https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/912728/000091272821000005/fwrd-20210203.htm

[iv] https://www.supplychaindive.com/news/cma-cgm-ocean-shipping-malware-cyber-attack-information-technology/585978/