2024

TRUCKING CYBERSECURITY TRENDS REPORT

NMFTA™
National Motor Freight Traffic Association, Inc.

INTRODUCTION

The trucking industry needs to stay prepared for cybersecurity threats in 2024. While some of the trends of 2023 will likely continue into the new year, no one is entirely prepared just from looking back.

The nature of this issue is that new threats emerge all the time while existing ones evolve. Part of our mission at NMFTA is to stay ahead of the game by keeping on top of research so we can anticipate what the industry is likely to face in the years to come.

This report presents some of our expectations on the cybersecurity front in 2024, as well as some insights from other organizations who also watch this issue closely.

PHISHING

Hackers frequently use phishing scams to gain access to a carrier's enterprise system. Once they can access the system, they use that access to launch ransomware attacks. Phishing attacks generally take the form of deceptive communications that trick people into clicking links or opening attachments.

Trucking companies' best preparation for, and defense against, these attacks is to thoroughly train their people on how to spot a phishing attack. Often phishing emails come from lookalike URLs, or from emails that pretend to be from known contacts. For example, a company might do business with Dell Logistics, with a domain of delllogistics.com. A phishing scammer might use the domain delllogistics.com. Spot the difference? The L in Logistics is a capitalized i.

Recipients should always look carefully at the sender's address to be sure the sender is really who it claims to be, and look carefully at links they are encouraged to click. Employees need to be trained that, when there is any doubt at all, they should not open attachments and not click on links.

API SECURITY

NMFTA will continue to focus on API Security on both the host and the mobile-side. Almost all trucking companies have host-side integration, which is a critical part of their workflow plan. In addition, the mobile side integration and telematics providers play a key role throughout the supply chain.

Cybersecurity experts cite several concerning API security. They include:

- The vulnerability of old, deprecated APIs known as Zombie APIs.
- Denial-of-service attacks that can overwhelm a website, server, or network.
- APIs that make it too easy for hackers to bypass authentication requirements.
- Accidental leakage of sensitive data, or exposure of stolen data.
- Undocumented back-door APIs known as "Shadow APIs".

DIRECT THREATS TO TRUCKS

With all the necessary attention of enterprise systems and the technology that supports them, we cannot overlook threats aimed directly at the trucks themselves.

As technology continues to evolve in the cab and everywhere around the truck, so does the potential for those elements to be compromised. In October, during our Digital Solutions Conference in Houston, TX we were able to demonstrate how a hacker could compromise the brakes on a truck by sending a message to the truck's diagnostic system using a simple antenna. On-board diagnostics and other telematics systems, as well as sensors can be used to wreak havoc if hackers can take control of them. In most cases, truck OEMs have not yet built in the factory-installed security measures that would provide the most security.

PREDICTIONS FROM OTHER VOICES

Some of our research on the subject of cybersecurity involves looking into the expectations of others who carefully watch this issue. To that end, we have aggregated some of the expectations from the following organizations:

Seattle-based WatchGuard forecasts that a smart prompt engineer – whether a criminal attacker or researcher – will crack the code and manipulate a Large Language Mode (LLM) into leaking private data.

While AI and Machine Learning (ML) risks may still only account for a fraction of the attacks during 2024, WatchGuard expects to see threat actors begin experimenting with AI attack tools and start to sell them on the underground.

WatchGuard also envisions an emerging market for automated spear phishing tools, or a combination of tools, on the dark web. Spear phishing is still one of the most effective tools attackers have to breach networks.

Also expected is an increase in Vishing, which is when a scammer calls a person pretending to be a reputable company or organization, or even a co-worker (or someone's boss), and urges the person to provide personal or sensitive data, or send money to a fraudulent account.

Another strong risk is an increase in QR code attacks. The convenience of QR codes is training people to unthinkingly do the very thing that cybersecurity professionals say they should never do, which is to click on random links without knowing where they go. Not only do QR codes encourage poor security practices, but they also obscure some of the techniques many would use to verify if a typical URL or hyperlink is safe to click on. With QR codes, attackers or scammers can trick users into visiting malicious sites or fool them by showing them things they can monetize, such as gift cards, discount coupons or cryptocurrency.

ARTIFICIAL INTELLIGENCE (AI)

As Artificial Intelligence (AI) takes the world by storm, it will have a serious impact – both positive and negative – on cybersecurity issues. Here is a summary of AI-related cybersecurity predictions from various other sources, including Gartner, Forrester, and Trend Micro:

- More effective cyberattacks than ever before against everyone, with bad actors leveraging GenAI (Generative AI) tools to find vulnerabilities in critical sectors.
- More AI threat actors, AI threat vectors, and AI code assistants will introduce further vulnerabilities *(BeyondTrust)*.
- Use of AI-based cyber defense is a must for enterprises to keep up.
- As many as 60 percent of workers engage in bring-your-own-AI (BYOAI) as their employers likely lack the tools internally but still want employees to leverage them. This has the potential to bring about serious security vulnerabilities. *(Forrester)*.
- Productivity improvements will drive rapid and widespread adoption of GenAI tools.
- Shadow AI will grow along with governance challenges.
- More regulations, laws, policies, data privacy, and ethics rules will emerge regarding appropriate use of AI. An uptick in sophisticated deepfakes and Business Email Compromise (BEC) will result from the use of GenAI to attack.
- More voice and video impersonations will appear, including accents and the targeted takeover of executive and personal social media accounts.
- An increased focus on various attacks against LLMs.

ELECTION THREATS

Election cyberattacks globally will be center stage. Specifically:

- Misinformation on elections in social media.
- Voting machine and virtual cyberattacks.
- Data surrounding voter lists, people, processes and technology cyberattacks.

GOOGLE CLOUD/MANDIANT PREDICTIONS

Here are some predictions concerning Google Cloud/Mandiant:

- Continued use of zero-day vulnerabilities.
- Cyber activity targeting U.S. elections.
- Rise of disruptive hacktivism.
- Wiper malware becoming a standard capability in all nation-state cyber arsenals.
- Targeting of space-based infrastructure.
- Attacks targeting hybrid and multi-cloud environments will mature and become more impactful.
- Serverless services in the cloud will be more heavily used by threat actors.
- Extortion operations continue.
- Espionage and “sleeper botnets”.
- Developers targeted in supply chain attacks via software package managers.
- Growing prevalence of mobile cybercrime.
- Cyber insurance premiums will remain steady.
- Consolidation around Security Operations (SecOps).
- Security gaps in cloud environments will set the stage for successful cloud-native worm attacks.
- Data will be weaponized against fledgling cloud-based machine learning models.
- Generative AI will allow fraudsters to level up their social engineering lures in targeted attacks.
- Software supply-chain attacks will serve as a clarion call to protect suppliers’ CI/CD systems.
- Attackers will look to the blockchain for fresh hunting grounds and extortion plans.

CONCLUSION

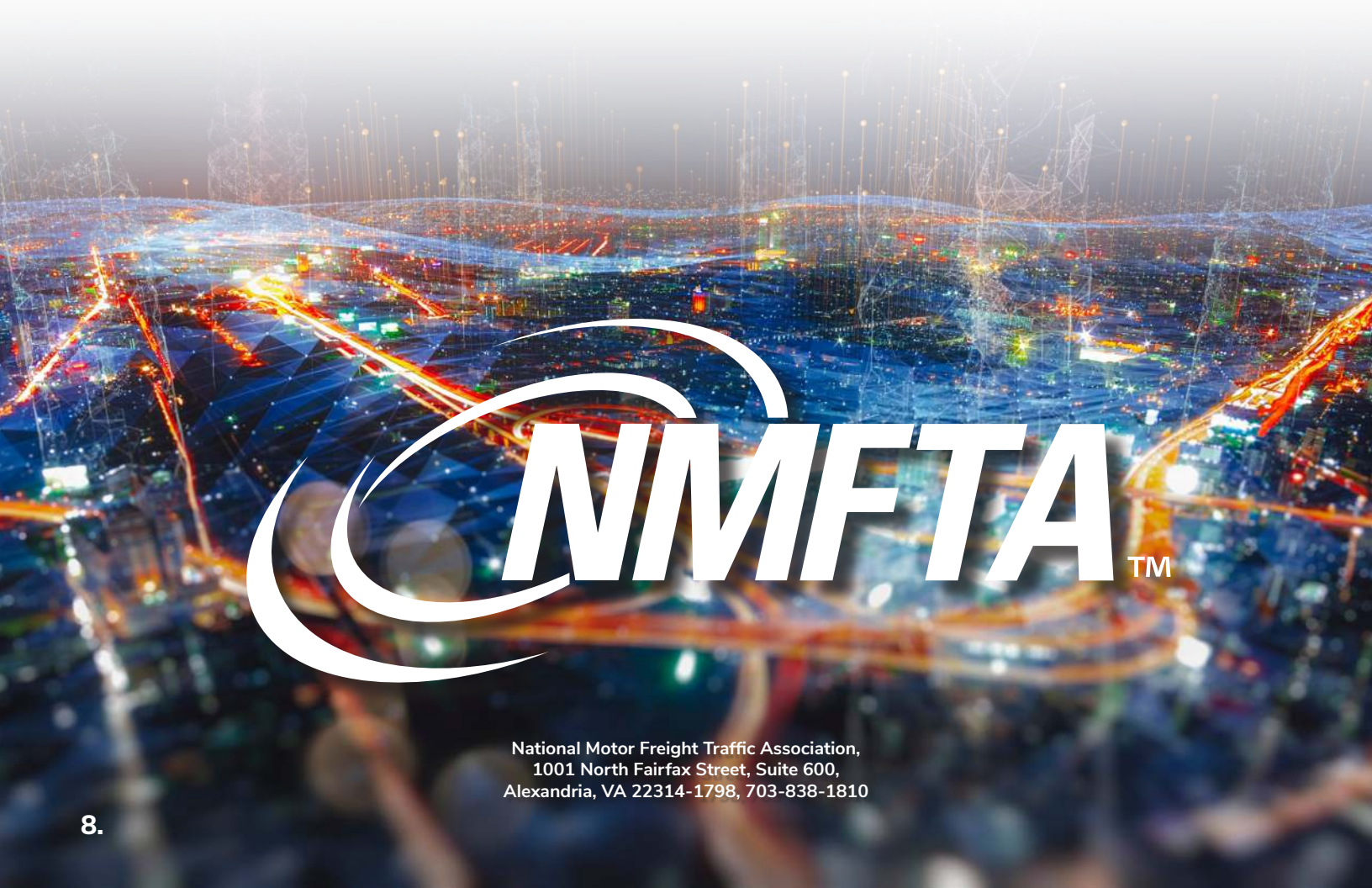
These trends and predictions highlight the evolving landscape of cybersecurity in 2024, emphasizing the critical need for proactive measures and advanced technologies to mitigate emerging threats. Cybersecurity professionals and organizations must remain vigilant and adaptable in the face of these evolving challenges.

NMFTA will be vigilant throughout 2024 about following these issues and sharing our findings with the industry. This effort will culminate, as always, with our annual three-day Digital Solutions Conference, which will take place this fall in Cleveland, OH.

During the 2023 conference in Houston, TX a wide variety of presenters from the private and public sectors – including critical players in the trucking industry – shared the latest insights on these evolving threats and the most effective steps to counteract them. We look forward to offering even greater value in 2024 to help the industry fight off cyberthreats.

To learn more about how you can protect your fleet or company, contact NMFTA's team of cybersecurity experts at cyber@nmfta.org.

For timely resources, http://www.nmftacyber.com/.



National Motor Freight Traffic Association,
1001 North Fairfax Street, Suite 600,
Alexandria, VA 22314-1798, 703-838-1810