A Collision From Afar: Cybersecurity Meets The Trucking Industry

William B. Pentecost, Jr., Esq.*

Henry J. Sienkiewicz, M.S.**

David M. Olive, Esq.***

It wasn't so long ago that the trucking industry security was focused on physical security and mechanical security. Companies wanted to prevent unauthorized vehicle use and to avoid a mechanical failure. The days of being simply focused on physical and mechanical security are long gone. Truck safety is now much more expansive.

Striving to be more effective and efficient, the trucking industry has embraced myriad digital technologies, from integrated fleet management systems that encompass maintenance management, GPS enablement, profit per mile calculations and fleet set-up, to "smart devices," which allow for GPS enablement, driver tracking and profiling, fuel consumption.

Cybersecurity is the industry's next waystation. The embrace of digital technologies makes it crucial to prioritize cybersecurity measures to protect the industry from the ever-evolving cyber threats and vulnerabilities. Through the adoption of robust cybersecurity strategies, the trucking industry can ensure the integrity, availability and confidentiality of critical data and systems, paving the way for a secure and efficient future.

The United States Department of Transportation (DOT) provides a great deal of guidance to the industry, subjecting the industry to its comprehensive Federal Motor Carrier Safety Regulations[1] that aim to ensure safety, efficiency, and compliance. These regulations and frameworks govern safety, environmental impact, and driver qualifications; but they do not fully address cyber security.

There has been significant research in this area. Earlier this year, the European Union Agency for Cybersecurity (ENISA) published its first cyber threat landscape report dedicated to the transport sector.[2] It found that ransomware attacks had become the most prominent threat against the transportation industry in 2022, with attacks having almost doubled from the previous year. Ransomware attacks were followed by data-related threats, as cybercriminals targeted credentials, employee and customer data, as well as intellectual property, for profit. More than half of the incidents observed in the past year were linked to cybercriminals, most of whom appeared to employ "follow the money" as their *modus operandi*. Attacks by hackers were also on the rise, with a focus on the geopolitical environment and the goal of operational disruption. The threats in the European trucking sector were predominantly ransomware attacks, followed by data-related threats and malware. The automotive industry, especially OEM and tier-X suppliers, has been targeted by ransomware, which has led to production disruptions. Data-related threats primarily target IT systems to acquire customer and employee data as well as proprietary information.[3]

Last year, the transportation and trucking industry was the ninth most targeted for cyberattacks.[4] It is not unusual for a trucking company's dispatching software to be hacked, so as to disrupt driver communications and reducing the company's ability to invoice for its services.[5] Cyber criminals have also set up fake loads of items to be transported and have diverted funds away from legitimate transactions. More mundane attacks include exploiting the diagnostics ports found in truck engines that are used to access telematics and diagnostic information for routine maintenance and repairs. Cyber criminals have become adept at using that connection to bring about a "denial of service attack," *i.e.,* preventing legitimate users from accessing information systems, devices, or other network resources.[6] A single cybersecurity

* Partner, Cipriani & Werner, P.C. (Pittsburgh, PA); Chair, TLA Motor Carrier Committee.
** Adjunct Lecturer, Georgetown University's School of Continuing Studies (Washington, D.C.)
*** Of Counsel, Cipriani & Werner, P.C. (Washington, D.C.); Principal, Catalyst Partners (Washington, D.C.).

disruption has the potential to cripple even the largest trucking companies while having a detrimental impact on the supply chain as a whole.

The efficiency of a trucking company's operations often presents the greatest opportunity for a cyber breach. Motor carriers ranging from the smallest to the largest in the industry typically have integrated their communications, billing, and logistics operations into a single database.[7] While advancements in GPS navigation and automated systems further enhance a company's operations, maintaining such varied applications in one place gives cybercriminals the chance to disrupt the business's supply chain in one targeted attack.[8]

Such attacks aimed at a trucking company may manifest in many forms. Phishing targets employees directly by falsely posing as a customer, public official, or even someone within the organization. Depending on the company's preparedness, ransomware and malware can bypass the firewalls and access confidential company and employee data. Even the rise of autonomous vehicles poses cybersecurity risks as their software can be hacked, leading to a loss of control over the vehicle and potentially damaging property and employees. Data theft was the most common outcome of these attacks, followed by extortion and impacts on brand reputation.[9]

In 2017, FedEx suffered a significant malware attack that limited its operations for months. More recently, Expeditors International of Washington, Seattle-based logistics giant, suffered a cyberattack that shut down most of its operating systems, diminishing its ability to conduct its operations, which was significant, given that it manages freight movements by air, sea and ground transportation in over three hundred locations around the world. Smaller fleets are likewise vulnerable, as cybercriminals accomplish their goal of causing panic by halting operations. [10]

Last year, Bay & Bay Transportation, a Minnesota trucking and logistics company, fell victim to a ransomware attack. The company was targeted by a ransomware gang known as "Conti," a so-called ransomware as a service provider, as it provides malware, an extortion platform and support to affiliates, who get a percentage of the payments made by victims. Conti has been linked to hundreds of attacks, including multiple transportation and logistics companies throughout the United States. While the attack impacted some of Bay & Bay's systems, including a small minority of its desktop computers, the company shut down all operations as a precaution. Unfortunately, this was the second cyberattack leveled against Bay & Bay in three years, but the prior experience led to the company employing measures, including network segmentation, to minimize the impacts of this attack, allowing the company to return to "90% functionality" within about a day and a half of the incident. The company credited quick action, training and cloud-based backups with enabling a rapid recovery.[11]

Bay & Bay, which has a fleet of over four hundred power units, disclosed the attack after Conti began posting data stolen from the company to the dark web. Groups like Conti typically do this after victims refuse to pay their ransom demands. The carrier was attacked through a known vulnerability in a Microsoft Exchange server. While Microsoft released an update a month earlier, which would have fixed multiple security issues, Bay & Bay had not run the update prior to the attack.[12]

The government and industry have not idly stood by. The US Department of Homeland Security (DHS), DOT, and industry organizations have done a great deal of research on these topics and have published guidance, which should be the industry's best practices.

There has been protracted debate as to what aspect of the infrastructure is the most critical.[13] While that debate continues to rage, the Department of Homeland Security has determined that the transportation and logistics industry is among the most critical to the infrastructure of the United States.[14] The government has determined that the protection of our logistical assets against cybersecurity attacks is of paramount importance, reasoning that transportation disruptions, such as an attack on logistical assets, can prevent the delivery of fuel, food, pharmaceuticals and raw materials, the interruption of the supply of any of which would be disastrous to our security and economy.[15]

The National Infrastructure Protection Plan (NIPP)[16] is a framework developed by the Department of Homeland Security to enhance the security and resilience of critical infrastructure sectors in the United States. Within the scope of the NIPP is a 2015 Transportation Sector Specific Plan (SSP)[17] focused on securing and ensuring the reliability of the transportation systems. Key components of the SSP include:

1. **Risk Management:** Highlights the need for risk assessment and management practices.
2. **Information Sharing:** Emphasizing the importance of information sharing and coordination among stakeholders and establishing information sharing networks and partnerships.
3. **Physical Security:** Addresses physical security measures to protect from threats such as terrorism, sabotage, and other malicious activities, to include security enhancements for critical assets, access control measures, surveillance systems, and the implementation of security protocols and procedures.
4. **Resilience and Continuity of Operations:** Emphasizes the importance of building resilience within the transportation sector, including strategies for maintaining essential operations, continuity planning, and the integration of resilience principles into infrastructure design and development.
5. **Cybersecurity:** Acknowledges the need for robust cybersecurity measures, to include the development of cybersecurity strategies, incident response plans, and the adoption of best practices to protect transportation.[18]

More recently, DOT published a draft

2020 draft update entitled, "Cybersecurity Best Practices for the Safety of Modern Vehicles."[19] An update to the 2016 document, the draft "is intended to cover cybersecurity issues for all motor vehicles and motor vehicle equipment (including software).[20] While not prescriptive, it does recommend that "(t)he automotive industry should follow the National Institute of Standards and Technology's (NIST) document Cybersecurity Framework,"[21] and, further, that the approach should:

- be built on risk-based prioritized identification and protection of safety-critical vehicle control systems;
- eliminate sources of risk to safety-critical vehicle control systems were possible and feasible;
- provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- design-in methods and processes to facilitate rapid recovery from incidents when they occur; and
- institutionalize methods for accelerated adoption of lessons learned.[22]

Finally, at a very high level, the DOT document outlines a specific vehicle development process with explicit cybersecurity considerations. This includes:

- process;
- risk assessment;
- sensor vulnerability risks;
- protections;
- inventory and management of software assets on vehicles;
- penetration testing and documentation;
- monitoring, containment and remediation;
- data, documentation and information sharing;
- continuous risk monitoring and assessment; and
- industry best practices.[23]

Established in 2015, the Automotive Information Sharing and Analysis Center (Auto-ISAC, Inc.) is an industry organization focused on enhancing cyber security in the automotive sector.[24] Recognizing that as vehicles become increasingly connected and, eventually autonomous, the manufacturers and suppliers recognized the need to provide safeguards from potential cyber threats that could compromise safety, privacy, and data integrity. It has developed a comprehensive set of best practices: incident response; collaboration and engagement; governance; risk assessment and management; awareness and training; threat detection; monitoring and analysis; and security development lifecycle.[25]

The regulations and guidance promulgated by DHS, DOT, and Auto-ISAC, Inc. are leading the industry to a cyber standard of care. *Standard of care* refers to the level of care, diligence, and responsibility that individuals and organizations are expected to exercise in the execution of their duties or protecting their assets. The notion of a cyber standard of care applies this concept to the principle of level of care, diligence, and responsibility to digital assets, information systems, and data from cyber threats and vulnerabilities.[26]

With the initial parameters set by the governmental agencies, then, this is the opportune time to establish a standard framework and benchmarks for a *cyber standard of care*, to consider the reasonable and prudent actions to prevent, detect, and respond to cyber-attacks and data breaches. This framework and benchmark should be grounded in current industry best practices, although reinforced by regulatory guidance and other providers, such as the insurance industry. Further, a *cyber standard of care* needs to be reasonable and prudent. The cybersecurity landscape is constantly changing and evolving, and organizations only have limited resources that they can devote to cybersecurity. The standard of care acknowledges that there is no one-size-fits-all solution and that measures must be tailored to the specific circumstance and organizational risk profile. There are several key principles that should be included in an evolving *cyber standard of care:*

1. **Risk assessment:** Organizations should conduct regular risk assessments to identify and evaluate potential cyber risks and vulnerabilities. This includes assessing the value of assets, likelihood of threats, and potential impacts.
2. **Security controls:** The implementation of appropriate security controls and safeguards is essential. This includes measures such as firewalls, intrusion detection systems, encryptions, strong authentication mechanisms, and regular software updates.
3. **Employee Training and Awareness:** Organizations must invest in educating and training employees about cybersecurity best practices, to include awareness about common threats like phishing, social engineering, and malware, strong password management, data handling practices, and reporting suspicious activities.
4. **Incident Response and Recovery:** A well-defined incident response plan, including procedures, is essential. The plan should have protocols for detecting, containing, and mitigating the impact of cyber incidents, post-incident analysis, and implementing measures to prevent future occurrences.
5. **Supply-chain Risk Management:** Organizations often rely on third-party vendors, suppliers, and partners for various services and solutions. A cyber standard of care requires that organizations assess and manage the cybersecurity practices of these third parties.
6. **Compliance with laws and regulations:** While the trucking industry is well-versed in compliance, the cyber security standard of care includes compliance with industry-specific standards, data protection

requirements, industry compliance frameworks, and contractual obligations.

7. **Continuous Monitoring and Improvement:** Cyber security is not a one-time checklist activity; it requires continuous monitoring, assessment and improvement of cybersecurity measures.

The industry's implementation of a cyber standard of care should include, at a minimum, current industry best practices, which include the use of a threat modeling, supply chain risk management. The adoption of a verified-trust approach should be the starting point.[27]

Threat modelling is the systematic identification of organizational assets, generally the assets believed to have value, *e.g.*, value to the attacker, value to the organization, or value as a stepping stone to something else. The model then identifies what the organization has, or is building, what can go wrong, and what should be done about it.[28] The threat model should be used in conjunction with the MITRE[29] Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework (MITRE ATT&CK Framework) and DHS's Cyber Security Evaluation Tool (CSET)[30] in order to provide a comprehensive view of the organization's entirety.[31]

A comprehensive understanding of the supply chain will also help identify and mitigate risk. The United States Department of Defense (DOD) defines Supply Chain Risk Management (SCRM) as the "systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DOD's 'supply chain' and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (*e.g.*, initial production, packaging, handling, storage, transport, mission operation, and disposal)." SCRM has four aspects: security, integrity, resiliency, and quality of information.[32]

Finally, the use of verified-trust principles during the implementation and operation phases. The idea of verified-trust is modification of NIST's Zero-Trust approach, and uses the principles of "verify, least privilege, micro-segmentation, assume breach, continuous monitoring, encryption, comprehensive access controls and automation."[33]

Like the situation with so many other industries, the vast majority of transportation companies will have great difficulty preventing all cyberattacks, particularly when those attacks are initiated or sanctioned by nation-state actors.[34] Cyber attackers will look for the weakest link into networked systems. Some of the most destructive attacks have started with an unprotected entry into a small business' computer system that is connected to a larger system. (*e.g.*, a targeted breach via a truck's diagnostic port). For that reason, many companies mitigate that risk by purchasing cyber security insurance. Cyber insurance policies may have significant differences in the language of what is covered, so transportation company risk managers should pay close attention to what risks they are retaining and what will be covered by their policies.

Moreover, recent decisions by major re-insurer companies to limit, if not outright exclude, coverage for ransomware attacks, as but one example, have created a level of uncertainty into mitigation strategies. The current situation is akin, although not identical, to the situation property and casualty insurance companies faced in the aftermath of the September 11, 2001, terrorists' attacks. Most private insurers took steps to exclude coverage for damages caused by terrorist attacks, leading Congress to create a federal Terrorist Risk Insurance as a backstop to shore up the private sector's willingness to cover terrorist-inflicted damages. The day before the Terrorist Risk Insurance Act received approval, Congress passed the Homeland Security Act of 2002, creating the Department of Homeland Security and, within it, a risk-mitigation program called the Support Antiterrorism by Fostering Effective Technologies Act of 2002, commonly known as the "SAFETY Act," to be administered by the DHS Science & Technology Directorate.[35]

The SAFETY Act[36] provides important legal liability protections for providers of Qualified Anti-Terrorism Technologies – whether they are products or services. The program's goal is to encourage the development and deployment of effective anti-terrorism products and services. Liability protections over the past 20 years have been extended to "sellers" of physical products and cyber protection systems. The SAFETY Act is specifically intended to provide liability protection to private sector entities where there is a terrorist caused act, and the determination of what constitutes an "act of terrorism" is made by the Secretary of Homeland Security. The definition of "terrorism" for purposes of the federal Terrorist Risk Insurance program is made by a group of three federal cabinet officials. Risk managers therefore should be aware of what their cyber security and terrorism risk insurance policies cover and, to the extent that there may be gaps in coverage, seeking SAFETY Act protections might be advisable.[37]

The SAFETY Act liability protections apply to a wide range of anti-terrorism products, systems, and services. A private sector entity must apply for protections for the Department of Homeland Security to determine if their offering is a Qualified Anti-Terrorism Technology.[38]

As a critical part of America's infrastructure, the trucking industry has been and will continue to be a target of cyber-attacks. Beginning well before, but accelerated greatly by the 9/11 attacks, the government has promulgated guidance and regulations to guard against such malicious attacks. These evolving standards serve as the baseline for the industry itself to develop and cyber standard of care, born of the industry's best practices, which have been and must continue to be ahead of governmental regulation and supervision. No cyber standard of care can be, nor should be expected to be, completely successful in preventing or repelling such attacks, so additional safeguards in the form of insurance are essential. The government encourages such pragmatism, as exemplified by the protections afforded by the SAFETY Act. Cyber attacks have become, and unfortunately will remain a frequent occurrence in the trucking industry.

Endnotes

1 49 C.F.R. Part 390.
2 ENISA Press Release, "Understanding Cyber Threats in Transport," https://www.enisa. europa.eu/news/understanding-cyber-threats-in-transport (last visited July 31, 2023).
"The ENISA threat landscape reports help decision-makers, policymakers and security specialists define strategies to defend citizens, organizations and cyberspace. This work is part of the EU Agency for Cybersecurity's annual work program to provide strategic intelligence to its stakeholders. Information sources used for the purpose of this study include open-source intelligence (OSINT) and the Agency's own cyber threat intelligence capabilities. The work also integrates information from desk research of available data such as news articles, expert opinions, intelligence reports, incident analyses and security research reports." *Id.*
3 *Ibid.*
4 Wombolt, S. and Shaw S. "A glitch on the road: cybersecurity trends facing the trucking and transportation industry." Web blog post. *MarshMcLennan Agency*, 04 May 2023. Online at: https://www.marshmma.com/us/insights/details/a-glitch-on-the-road-cybersecurity-trends-facing-the-trucking-and-transportation-industry.html. Accessed 11 Aug. 2023.
5 *Ibid.*
6 Wendt, R. "Protect Your Fleet Against the Growing Risk of Cyber Attack." Web blog post. HDT Trucking Info, 21 Dec. 2022. Online at: https://www.truckinginfo.com/10189293/protect-your-fleet-against-the-growing-risk-of-cyber-attack. Accessed 11 Aug. 2023.
7 *Supra*, note 4.
8 *Ibid.*
9 *Ibid.*
10 *Supra*, note 6.
11 Tabak, N. "Minnesota trucking company hit in 2nd ransomware attack." Web blog post. *Freight Waves*, 02 Jan. 2022. Online at: https://www.freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack. Accessed 11 Aug. 2023.
12 *Ibid.*
13 Jablanski, D. "Critical infrastructure cybersecurity prioritization: A cross-sector methodology for ranking operational technology cyber scenarios and critical entities." Web blog post. *Atlantic Council Cybersecurity*, 19 Apr. 2023. Online at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization. Accessed 11 Aug. 2023.
14 *Ibid.*
15 *Supra*, note 6.
16 See: CISA, *National Infrastructure Protection Plan and Resources*. Online at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources. Accessed 11 Aug. 2023.
17 CISA, *Transportation Systems Sector-Specific Plan – 2015*. Online at: https://www.cisa.gov/resources-tools/resources/transportation-systems-sector-specific-plan-2015. Accessed 11 Aug. 2023.
18 *Ibid.*
19 Cybersecurity Best Practices for the Safety of Modern Vehicles, 86 FR 2481, Docket No. NHTSA-2020-0087 (January 12, 2021).
20 *Ibid.*
21 *Ibid.*
22 *Ibid.*
23 *Ibid.*
24 Auto-ISAC, Inc. is located at 20 F Street NW, Suite 700, Washington DC 20001 and is accessible online at www.automotiveisac.com. Accessed 11 Aug. 2023.
25 *Ibid.*
26 *See, e.g.*, Cyber Crossroads. "Cyber Crossroads: A Global Research Collaborative on Cyber Risk." Online at: www.cybercrossroads.org. Accessed 11 Aug. 2023.
27 Sienkiewicz, Henry J. Perspectives in *Additional Cybersecurity*, March 15, 2023, Georgetown University MPTM 665.
28 Shostack, Adam. *Threat Modeling: Designing for Security.* 1st Edition, Wiley, February 17, 2014.
29 "MITRE" is not an acronym but a company name: www.mitre.org/who-we-are. Some mistakenly believe the letters stand for "Massachusetts Institute of Technology Research & Engineering." *See, e.g.*, www.xcitium.com/what-does-mitre-stand-for (last visited July ____, 2023).
30 Introduction to the Cyber Security Evaluation Tool and Modules, www.isao.org/resource-library/government-programs/dhs-cybersecurity-evaluation-tool-cset-and-on-site-cyber (last visited July 31, 2023).
31 *Supra*, note 27.
32 Sienkiewicz, Henry J. *Additional Perspectives SCRM*, April 15, 2023, Georgetown University MPTM 665.
33 See National Institute of Standards and Technology Special Publication (NIST SP) (800-207, 2023).
34 Although it is beyond the scope of this article, the authors recommend that attention be paid to the cybersecurity and liability issues arising out of the Massachusetts' "right-to-repair" law and the US Department of Transportation's recommendation that the law be ignored.
See www.thedrive.com/news/feds-tell-automakers-to-ignore-massachusetts-right-to-repair-law (last visited July 31, 2023).
35 *See, e.g.*: Finch, Brian E. and Spiegel, Leslie H. *Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety Act*. 30 Santa Clara High Tech. L.J. 349 (2014).
36 As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002. www.dhs.gov/science-and-technology/safety-act (last visited July 31, 2023). It should be noted that the SAFETY Act only applies to claims and cases subject to United States law; there is no presumption that the Act would be applied in jurisdictions outside the United States.
37 *Supra*, note 35.
38 *Ibid.*