IADC SUPERIOR ADVOCATES. GLOBAL PERSPECTIVE.

COMMITTEE NEWSLETTER

CELEBRATING 100 YEARS 1920-2020

TRANSPORTATION

DECEMBER 2019

In This Issue

*Heather Devine, Partner at Alexander Holburn LLP, outlines how private motor carriers, including members of the trucking industry, can be subject to data breach and cybersecurity issues. A cybersecurity threat can include both first party and third party costs. Businesses can be susceptible to financial risk, if hackers target customer or trade information, or electronic logging devices ("**ELDs**") data. There is also potential security threat of cyberattacks which target trucks with ELDs and the potential ability of hackers to controlling temperature gauges and accelerate vehicles remotely. Potential tactics used by cyber security may include use of malware, phishing and distributed denial of services ("**DDOs**"). There are significant insurance implications to these threats. A cyberattack will cause chaos and potentially significant first and third party liabilities, however, businesses can minimize impact by implementing risk management techniques and best practices as suggested in this article.*

Hacked or Cracked? A Practical Guide to Cybersecurity for Private Motor Carriers

About the Author

Heather Devine is one of Canada's leading transportation lawyers. From 2014-2020, she has been recognized as one of the *Best Lawyers*® in Canada for Transportation Law, and is the current President of the Canadian Transport Lawyers Association. Heather was admitted to the Ontario bar in 1999 and the Nova Scotia Bar in 1998, and has a J.D. law degree from Queens University. Heather worked as a commercial litigator until learning to fly single engine planes in 2009, which led her to focus in transportation law. Since then, her focus has included combining technology, transportation, and intellectual property to advise clients such as brokers, freight forwarders, carriers, and other clients who move goods locally and internationally. In her spare time, Heather flies airplanes and works as an instructor to perform simple aerobatics in the Pitts Special S-2A. She also rides motorcycles, including her Kawasaki Ninja. She can be reached at hdevine@ahbl.ca.

About the Committee

This IADC Committee was formed to combine practices of aviation, rail, maritime with trucking together to serve all members who are involved in the defense of transportation including aviation companies (including air carriers and aviation manufacturers), maritime companies (including offshore energy exploration and production), railroad litigation (including accidents and employee claims) and motor carriers and trucking insurance companies for personal injury claims, property damage claims and cargo claims. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Alan Polivnick
Vice Chair of Publications
Watson Farley & Williams
apolivnick@wfw.com

*The **International Association of Defense Counsel** serves a distinguished, invitation-only membership of corporate and insurance defense lawyers. The IADC dedicates itself to enhancing the development of skills, professionalism and camaraderie in the practice of law in order to serve and benefit the civil justice system, the legal profession, society and our members.*

***w:** www.iadclaw.org **p:** 312.368.1494 **f:** 312.368.1854 **e:** mmaisel@iadclaw.org*

Hacked or Cracked? Is Cybersecurity a real risk for Private Motor Carriers? The answer is: yes. Despite being a 10-year customer of a business, at checkout, while handing over my credit card, I was asked to provide all of my customer information *again* - name, address, phone number, and email. I was surprised and asked: "Why? I am already in your system…"
I learned the business's computer systems had been hacked and held for ransom for approximately $10,000. During the hostage negotiations, while the customer information was being held for ransom, the business contacted their insurer but learned that they had in fact declined Cyber liability insurance coverage (they told me they thought they were covered). Rather than pay the ransom, the business decided to purchase a new computer system (same price as the ransom), and to start from the beginning to compile customer information.

First Party and Third Party Losses=$$$

These losses for the business would constitute **First Party Losses**. In this incident, the cost of the new systems and security was the same as the ransom. However, all private information, data and customer contacts were gone. As a customer, I wondered: where is my customer information now? Locked in their old system? Available to criminals? Do I have redress? And why wasn't I told when it happened? I questioned: Can I sue?

Had I made a claim or sued, my claim or lawsuit would be a **Third Party Claim or Loss**. What would your business do? Pay the ransom and hope to get the customer information back intact? Walk away and buy a new system entirely, but lose all customer information? What about any obligation to tell the customers that their personal information had been stored in a system that had been hacked and ransomed? What about the security for the customer's new information? These issues are becoming more prevalent in the transportation industry: the risk is real -- so implement practical solutions and best practices to protect your business now, and ensure you purchase the appropriate insurance coverage -- before you need it.

Data breaches affect us daily

Data breaches affect us daily, and they pose a unique threat to the trucking industry. There are two areas where cybersecurity is of interest today: financial risk as exemplified above where a cyberattack affects the security of one's data -- where the data affected could include customer data, business information, and even stored ELD sourced data; and a cyberattack through accessing vehicles through the connectivity of trucks, which is a threat that will likely increase in magnitude in the future.

The First and Third Party Costs of a Cyberattack

The financial risk of a cyberattack, and the obligation to enact cybersecurity protection for stored data threaten Private Motor Carriers: this article focuses first on the financial risks of cyberattacks on stored and accessible data, then considers the more 'futuristic' (but real) issue of cyberattacks through connectivity (including ELDs), and ends with proposed best practices and insurance considerations.

Common cyberattacks: malware, phishing, DDos

The most common types of cyberattacks are:

- **Malware**: malicious software that is propagated with link clicks and attachment downloads.
- **Phishing**: fraudulent emails which steal information or encourage malware downloads.
- **DDos or Distributed Denial of Services**: multiple, simultaneous requests which bombard a business's server to prevent it from fulfilling legitimate requests.

Financial Risk of Common Cyberattacks on Customer, Trade Information or stored ELD Data

When business systems are breached or hacked, the business can incur costly containment and repair expenses. Affected third parties can bring lawsuits and exponentially increase unpredictable costs and damages arising from the breach. In these circumstances, a business must be prepared to act quickly and to follow protocols which provide stability and limit risk -- during the attack a business will strive to regain control and certainty which is almost impossible if a business is unprepared.

The motivations for an attacker can be numerous:

- Criminal efforts to make a profit from manipulating commercial data or vehicles
- Hijacking goods
- Adversely manipulating a competitor's fleet
- Extorting fleet owners and drivers
- Selling tools and services on the black market
- Terrorism.[1]

Security Risk of Trucks Being Accessed While En Route

> *"Easy access for safety-critical attacks"*

Before we consider the potential role of ELDs in cyberattacks, be advised that it is not just the software that leads to vulnerability. Several researchers proved that they were able to access, hack and affect the performance of commercial vehicles by attacking the J1939 protocol instead of the software.

> In *"Truck Hacking: An Experimental Analysis of the SAE J1939 Standard"* the authors conclude:
>
> *"We show how the openness of the SAE J1939*[2] *standard used across all US*

[1] Truck Hacking: An Experimental Analysis of the SAE J1939 Standard by Yelizaveta Burakova, Bill Hass, Leif Millar and Andre Weimerskirch, the University of Michigan, p. 5

[2] The authors note: All modern heavy duty trucks and buses in the United States use the SAE J1939 Standard (J1939) for their internal networks. "*While standardizing these communications has proven*

> *heavy vehicles industries gives easy access for safety-critical attacks that these attacks aren't limited to one specific make, model, or industry."*[3]

The attacks were not tested on autonomous vehicles: instead, the attacks were tested on a 2006 Class-8 semi-tractor and 2001 school bus. These are ordinary commercial vehicles - the risk is real.

The researchers proved they could accelerate a truck in motion, disable the driver's ability to accelerate, and disable the vehicle's brake. Given the age of the semi-tractor and school bus, it is clear that hacking into commercial vehicles to affect their operations is NOT the future: it is already here.

Heavy trucks increasingly employ systems with electronic control to increase stability and safety: such as electronically controlled antilock brake, anti-slip regulation, and active rollover protections systems. It is not necessary to project to a future with autonomous vehicles on the road to understand the risk of a cyber-attack through such every day systems.

Further, heavy trucks are typically part of a larger fleet of vehicles, which are monitored using fleet management systems (FMS). The FMS standard is a worldwide standard developed in 2002 which combines satellite and cellular communications to provide information about vehicle location and status. The FMS standard is designed to allow third party systems to integrate across manufacturers, and these third party devices can be a source of cyberattack. In some cases, the researchers found third party fleet management systems connected to the vehicle's internal network where the Telnet port was *wide open*.

The researchers launched attacks on the safety critical systems of heavy vehicles and attained success:

- They 'spoofed' the status messages originating in various Electronic Control Units (ECUs) of the truck and precisely controlled ALL gauges on the instrument cluster: oil temperature, oil pressure, coolant temperature, RPM, speed, fuel level, battery voltage, and air pressure of the of the foundation brake system.

- They were able to override the driver's input to the accelerator pedal and simultaneously cause either direct acceleration or remove the ability to provide toque to the wheels while the truck was in motion.

- They were able to disable the truck's ability to use engine braking at speeds below 30 miles per hour.

crucial in allowing various suppliers and manufacturers to work together and cut costs, it also means that all heavy vehicles currently on the road in the US, from semi tractor -trailers to garbage trucks and cement mixers to buses, utilize the same communication protocol on their internal networks."

[3] Truck Hacking: An Experimental Analysis of the SAE J1939 Standard by Yelizaveta Burakova, Bill Hass, Leif Millar and Andre Weimerskirch, the University of Michigan, in Usenix WOOT, August 11-12, 2016, Austin, TX, USA, p. 1

Do ELDs create new vulnerability?

Private Motor Carriers are well aware of the government mandate to institute the use of electronic logging devices or ELDs. The implementation of ELDs is often tied to safety and hours of service tracking, and the collection and storage of a driver's hours of service data, which is obtained by connecting to the engine, is commonly made by connection through a cellular data network.

There are many areas of potential vulnerability: both from hacking into the devices and affecting the operation of the vehicle, as well as accessing the company's collection and storage of collected data.

IoActive tested five different ELDs to identify vulnerabilities that could allow attackers to "pivot through the device and into the vehicle" with what is reported to be potentially disastrous results.[4] Urban Jonson, chief technology officer for the National Motor Freight Traffic Association, Inc. (NFMTA), reports:

> *"There is still significant concern regarding the cybersecurity posture of ELDs and their providers… In vehicle components have been found to lack in cybersecurity hygiene features such as secure boot, encrypted communications and privilege separation."*[5]

To allay concerns about ELD devices, manufacturers advise that ELD devices are not designed to write to the engine's control module, but are designed to receive and transmit data from it. ELDs reportedly also have various security measures in place.

Nonetheless, AT&T released a press release to announce that AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic joined forces in a new Alliance to innovate in the security space regarding providers of Internet of Things (IoT) devices. This announcement is significant to the Private Motor Carriers because ELDs are devices which must be included when examining IoT security challenges.

AT&T advised:

> *"In the past 3 years, AT&T has seen a 3,198% increase in attackers scanning for vulnerabilities in IoT devices.*

More specifically, AT&T Chief Security Officer Bill O'Hern said:

> *Be it a connected car, pacemaker or coffee maker, every connected device is a potential new entry point for cyberattacks …*
>
> *Yet, each device requires very different security considerations. It's become essential for industry leaders and innovators like those in the founding members of this Alliance, to work*

[4] "As the connectivity of trucking grows, so do cybersecurity risks" posted in General Security on April 10, 2019 https://resources.infosecinstitute.com/as the connectivity of trucking fleets grows so do cybersecurity risks/#gref

[5] "As the connectivity of trucking grows, so do cybersecurity risks" posted in General Security on April 10, 2019 https://resources.infosecinstitute.com/as the connectivity of trucking fleets grows so do cybersecurity risks/#gref

together to help the industry find more holistic security approaches for IoT"[6]

One solution, proposed by Jeremy Daily, PH.D. associate professor of mechanical engineering at the University of Tulsa, is a newly developed hardware device called CAN (Controlled Area Network) Data Diode. The CAN Data Diode works by preventing communication from the ELD to a commercial vehicle. However, this device is not yet commercialized, so it is not a practical solution for PMCs in Canada at this time.

Best Practices are the First Step

To manage risk and limit liability, a Private Motor Carrier can implement best practices and insure against the first and third party losses that can ensue. Here are a few best practices collected from a variety of sources.

- Assess risks and the nature of identified threats and vulnerabilities through a defined process consistent with your overall risk-management strategy.

- Use threat monitoring to understand current and emerging threats and reduce enterprise risk.

- Implement routine scanning and testing of the areas of highest risk - evaluate whether you can disable or remove features that enable remote access to a third party, such as diagnostic services, when not in use.

- Establish and follow procedures for identifying, measuring and prioritizing cybersecurity risks - stay up-to-date with security providers, communications and software system updates.

- Establish and follow an incident response plan (IRP) which includes processes for identification and containment through remediation and recovery.

- Establish an incident response team (IRT).

- Conduct and document regular testing and coordinate the testing with the incident response team (IRT) and update and modify the IRP to reflect the results obtained by regular testing.

- Establish training procedures which includes the IRT and well as operations, risk management, and IT personnel.

- Locate and purchase applicable insurance, verify coverage, and work with your broker and or insurance provider to ensure that the best practices employed match your coverage.

- Consider implementing provisions regarding the impact of cyberattacks into shipper-carrier and broker-carrier

[6] https://www.overdriveonline.com/cybersecurity-alliance-formed-specifically-to-address-iot-the-internet-of-tru-um-things/; citing "Cybersecurity alliance formed specifically to address IoT, the Internet of Tru…um, 'Things'" Channel 19, Todd Dills, February 13, 2017 at overdriveonline.com

agreements to manage risk by limiting liability (first and third party) and avoiding or reducing economic losses.

Cyber liability Insurance Provides Protection: Know Your Coverage

Cyber liability insurance covers two main areas of risk First and Third-Party Insurance: First-party insurance provides coverage for direct costs associated with responding to the failure and managing the incident. Third party insurance provides coverage for lawsuits or claims that arise as a result of the cyber incident.

Make sure you get a clear explanation of what is covered in your insurance policy and what is excluded; for example, when reviewing coverage assess whether it covers

- breach assessment and repair;
- business interruption and/or economic losses;
- ransom payments;
- reputation management;
- third party legal fees and settlements; and
- perhaps even regulatory fines.
- Some policies may even include marketing costs to recover a business's reputation.

However, Technology E&O (errors and omission) coverage does not provide protection against cybercrimes.

Consider too that you must specifically purchase Cyber extortion coverage to provide coverage for a consultant or negotiator, or repair costs of the recovered data is locked or damaged.

Conclusion

In summary, whatever the nature of the cyberattack (financial or more rarely, through connectivity with commercial vehicles), it is important to understand that the attack, when it happens, will cause chaos and potentially significant first and third party liabilities.

In order to limit the potential damages, and ensure that your business retains control during the attack, implement best practices which match your business' risk management profile, and ensure that you have sufficient insurance coverage.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

NOVEMBER 2019
The Case of the Haphazard Switcher: Missouri Appellate Court Renders Disturbing Interpretation of "In Use" Affirming an Injury-Prone Railroader's SAA Verdict
J. Mitchell Smith

SEPTEMBER 2019
A Railway Bridge Too Far: A Struggle between FELA and LHWCA
J. Mitchell Smith

FEBRUARY 2018
Thailand Ratifies Montreal Convention
Alan Polivnick, Kulkanya Vorawanichar, and Nicharee Musikapraphan

MARCH 2017
Ready or Not, Here it Comes: How Current Regulations Must Adapt to the Development of Driverless Trucking Fleets
Brett M. Simon and Mary Anne Mellow

FEBRUARY 2017
The Duty to Preserve Electronic Evidence in the New Age of Transportation Under Amended FRCP 37(e)
Larry Hall and Mary Anne Mellow

DECEMBER 2016
New Overtime Rules Mean Change is Coming for all Employers – Transportation Industry Included – or Do They?
Larry Hall, Amanda N. Johnson, Mary Anne Mellow and Narcisa Symank

NOVEMBER 2016
General Jurisdiction via State Registration Statute – Consistent with Daimler? – Part II
Nancy M. Erfle, Amanda N. Johnson, Mary Anne Mellow and Steve Walsh

OCTOBER 2015
General Jurisdiction via State Registration Statute – Consistent with Daimler?
Mary Anne Mellow, Michele Parrish and Nancy M. Erfle

SEPTEMBER 2015
Recent Regulatory Interpretations and Court Decisions on the Employment/Independent Contractor Relationship between Drivers and Transportation Network Companies
Donna L. Burden and Andrew J. Kowalewski

AUGUST 2015
Transportation Network Companies: Recent Regulatory Challenges and Proposed Regulations
Donna L. Burden and Andrew J. Kowalewski