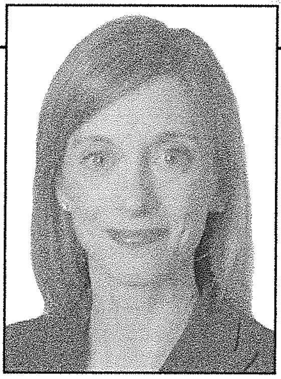
Electronic Logging Devices ("ELDs"): *Yet Another Avenue for a Cyber Attack?*

Molly Arranz*



On an already busy afternoon, your operations manager gets a call from a driver. She is stuck in the middle of a highway because her truck died without warning. Weather has already caused a delay and the delivery date was essentially yesterday. Scrambling ensues and the operations team springs to action as they speed dial the standard roadside supports.

However, a review of mechanical failures, flat tires and the like reveals no solution that can be readily implemented. As the operations manager is scratching his head, he gets an e-mail. It is a demand for $50,000 in bitcoin from some hacker named SamSam. If the company does not pay the "money," the truck stays dead and the delivery of the shipment does not happen.

Could this scenario really happen? Ransomware attacks have been in the news for years now but perhaps you relegate these cyberattacks to headaches for the financial and healthcare sectors. You shouldn't. You should be wary of these types of cyber threats given the increasing technology *mandated* in the trucking industry together with the growing sophistication of hackers who could take your system for "ransom."

A traditional ransomware attack looks like this: an employee receives what seems to be an innocuous e-mail from a familiar name. He clicks on the attachment and his computer goes haywire. Other employees try to access files for their daily work, but they are prompted for a password, or 'key.' Another e-mail is received wherein a hacker demands a large sum in bitcoin. How did this likely happen? A hacker targeted an employee with access to the company's network files with a phishing e-mail. Opening that e-mail opened a door for the hacker, who had malware at the ready. The hacker then encrypted, or locked-up, the network–and he has the only key.

You may have heard of the ransomware attack on TNT Express, where hackers exploited a vulnerability in a software update. During the attack, hackers used a strain of malware called NotPetya to lock the company's systems; they demanded a hefty cryptocurrency payment to cure it.[1] The hack resulted in widespread service delays and posed significant operational challenges for the company.[2] Although the hackers did not access or exfiltrate the data, a very real impact was felt in the form of disruption of TNT Express's systems and deliveries. The company had to revert to manual business processes to remain operational. And, most significantly, it reported a $300 million loss in earnings–together with costs that it incurred to fully restore all of its global and IT operations at its facilities, hubs, and depots, as a result of the attack.[3]

Cyberattacks will likely be on the rise and come from all directions because today's vehicles have increasing, and multiple, electronic devices and units. Each device and unit could serve as a potential door to hacker infiltration. High-tech navigation systems, communication channels and, now, electronic logging devices ("ELDs") are all possible entry points, especially when coupled with a workforce that has varied levels of training and who spends the majority of its time behind the wheel relying on instincts while trying to meet deadlines or timetables.

This article will present a discussion of key cybersecurity issues pertinent to just one of these potential security gateways–ELDs. First, by way of background, it will provide an overview of the ELD Mandate's requirements, which are set to go into full effect this December. It will further provide an overview of state and organizational responses to the ELD Mandate. Second, it will provide an analysis of the cybersecurity risks that ELDs pose and of cyber incidents involving analogous technologies in the realm of commercial and consumer vehicles. Finally, it will present concrete steps and resources that trucking companies should consider in order to reduce the likelihood of falling victim to potential cyber-attacks.

I. ELDs and the ELD Mandate

The DOT certified ELDs as the go-to and required hardware technology, meaning, the technology itself becomes essentially a part of the truck. In the past, ELDs were referred to as automatic on-board recorders ("AOBRDs"). These devices automatically record a driver's driving time, in order to allow truckers and trucking companies to record, more easily and accurately, the driver's hours-of-service ("HOS").[4] An ELD could be a smartphone, tablet or laptop. The devices are meant to replace the paper log book systems that drivers previously used to track their hours.[5]

The hardware for ELDs connects to the vehicle's engine to record driving hours and includes a screen for the driver to monitor his or her current status.[6] ELDs are connected to fleet management software, which allows for the transmission of real-time driving

*SmithAmundsen LLC (Chicago, Illinois)

logs to the trucking company's back-office system.[7] The transmission of driving logs is facilitated by the ELD's connections to the Internet and cellular data networks.

i. *The ELD Mandate*

In December 2015, the Federal Motor Carrier Safety Administration ("FMCSA") mandated that all truck drivers use ELDs in place of paper log books. The ELD Mandate was issued as part of a Congressional initiative to increase highway and transportation safety and to help monitor compliance with HOS requirements.

The ELD Mandate has been implemented in three phases. The first phase of enforcement ended on December 18, 2017, and applied to carriers which did not have any system for recording HOS. Specifically, these carriers had until December 18, 2017, to adopt either AOBRDs, logging software, paper logs, or certified ELDs which were registered with the FMCSA and compliant with published specifications under 49 C.F.R. 395.15.[8]

The second phase of enforcement is in progress and ends on December 16, 2019. By this date, all carriers must be equipped with either AOBRDs (provided they were installed and in-use before December 18, 2017) or certified ELDs which are registered with the FMCSA and compliant with published specifications under 49 C.F.R. 395.15.[9]

The final phase of enforcement begins on December 16, 2019. From this date, all carriers must have only certified ELDs which are registered with the FMCSA and compliant with published specifications under 49 C.F.R. 395.15. All AOBRDs, logging software, and paper logs will be phased out.[10]

ii. *Response to ELD Mandate and Continued Enforceability*

Although the ELD Mandate is federal law, some states have been hesitant to adopt it. Specifically, in 2018, Tennessee, Missouri, Wyoming, Idaho, Alabama, and South Dakota introduced legislation to *undermine* the ELD Mandate.[11] In South Dakota, lawmakers called on the FMCSA to review the ELD Mandate and to collaborate with the trucking industry to develop a reasonable solution and modify existing regulations, instead of creating new ones.[12]

Other opponents of the ELD Mandate have included the Owner-Operator Independent Drivers Association ("OOIDA"), which lobbied Congress to delay the rule's implementation for small carriers. Specifically, in August 2017, OOIDA members complained that state law enforcement agencies were unprepared to comply with the ELD Mandate, which was to become partially effective that December. They pointed to legal issues presented by state enforcement of the ELD Mandate, since certain states had not formally adopted the federal safety standard.[13]

In fact, in 2018, the OOIDA filed a lawsuit challenging the state of New York's enforcement of the ELD Mandate. Notably, the OOIDA alleged that the state's officers were issuing citations to carriers and drivers for not having ELDs installed, *even though* the state had not adopted the ELD Mandate. The highest court found that state officers could not enforce the ELD mandate until it was codified into New York law.[14]

On the other hand, supporters of the ELD Mandate include the Commercial Vehicle Safety Alliance ("CVSA"). In 2017, the CVSA advocated for the rule's enforcement because supporting research from the FMCSA showed that carriers' use of ELDs reduced crash rates and truckers' HOS violations.[15] Moreover, Colin Mooney, Executive Director of the CVSA, maintained that there was sufficient time for carriers to comply with the ELD Mandate's requirements. Specifically, he stated that two years was adequate time for carriers to obtain ELDs for their vehicles.[16]

Despite the controversial nature of the ELD Mandate, the FMCSA retains the authority to ensure that states enforce it.[17] Thus, you can and should expect the ELD Mandate to be enforced–state-by-state.

II. Concern Over Vehicle Systems Being Hackable

In the end, since the ELD Mandate requires all commercial vehicles to have an ELD hardwired into, and synchronized with, the vehicle's engine, a fleet's chances of suffering a ransomware or other cyber attack–via this new gateway–is a real possibility.

Perhaps you resist such a premise because there is currently no evidence of a malicious hack through a company's ELDs. But consider the potential (increased) vulnerabilities that such technology–thread through the hardwiring of the truck itself and using programmable software–may introduce. In fact, past research and testing of the computer systems for vehicles may be instructive on the cyberattack possibilities.

In 2015, two cybersecurity researchers, Charlie Miller and Chris Valasek, were able to hack into the system of a 2014 Jeep Cherokee remotely because of vulnerabilities in the car's software. Through the internet, they hacked into the Jeep's control area network to access the car's entertainment features and navigation system.[18] The researchers exploited weak points in the system and infiltrated it by running code. Once they were "in," they controlled anything that was connected to the software features of the car: the steering, the brakes, lock-and-unlock features and transmission. Upon these findings, Chrysler issued a software fix and recalled 1.4 million vehicles at a cost of approximately $140 million[19] in order to upgrade the vehicles software and prevent future attacks.[20]

Similarly, researchers at the University of Michigan conducted a study in 2016 to assess the security of software used in commercial motor vehicles. They were able to successfully hack the SAE J1939 standard[21] of a 2006 semi-trailer and were able to send commands to change the readouts of any part of the trailer's instrument panel. Specifically, they had the ability to prevent a driver from seeing an alert indicating that the truck was about to run out of compressed air in its tires. They also had the ability to prevent him from fully disabling the truck's engine brakes.

Taking just these two, controlled "hacks" in combination with the adoption of recently-required technologies like ELDs shows how seriously you should consider the access points to your entire system–and business. With the increasing sophistication and greed of hackers who only have time on their hands, cyber security concerns will persist and, likely even, increase with the adoption of recently-adopted technologies like ELDs.

In fact, members of the National Motor Freight Traffic Association have already expressed concerns about the security of ELDs, generally, and complained that these risks are not addressed within the ELD Mandate as a whole.[22]

III. Steps that Carriers Should Take to Protect Themselves from Cyber Incidents

With this, there is a very real possibility that a hacker could open one of multiple doors to access and control not only the vehicle's data but, possibly, the company's entire system. An intrusion into just one truck's system could have a domino effect, costing time and money by the hour, day or longer.

There are preventative measures that carriers should take to minimize their risk. First, carriers should keep their operating systems updated with the latest software updates. Second, carriers should install and maintain anti-virus programs to screen communications and ensure that unauthorized communications do not come through. Third, carriers should evaluate their drivers' and employees' respective levels and access to the company's databases. Fourth, carriers' operations teams should conduct back-ups of their systems and critical data to an offline server. This will allow the server to be of use for restoring any lost data after the wiping of impacted systems. And finally, train, train, train. Carriers should make data security part of their onboarding orientation and regular training for all employees and drivers to help protect against data incidents from suspicious communications and ransomware attacks.

Endnotes

[1] Gary Frantz, *Cyber Defenders: How Fleets are Preventing Hackers from Disrupting IT Systems, Stealing Data,* Transport Topics (Apr.20, 2018, 1:45PM), **https://www.ttnews.com/articles/cyber-defenders-how-fleets-are-preventing-hackers-disrupting-it-systems-stealing-data**.

[2] *Id.*

[3] *NotPetya cyber-attack cost TNT at least $300m,* BBC News (Sept. 20, 2017), **https://www.bbc.com/news/technology-41336086**.

[4] *What is an electronic logging device (ELD)?,* Federal Motor Carrier Safety Administration, (Dec. 10, 2015), **https://www.fmcsa.dot.gov/faq/what-electronic-logging-device-eld**.

[5] Earline Gloss, *The ELD Mandate 101: What Drivers and Carriers Should Know,* Logistic Dynamics, (Dec. 28, 2017), **http://www.logisticdynamics.com/eld-mandate-facts**.

[6] *What is an ELD,* Verizon Connect, (2019), **https://www.verizonconnect.com/glossary/what-is-an-eld**.

[7] *Id.*

[8] *Implementation Timeline,* Federal Motor Carrier Safety Administration, (Dec. 24, 2018), **https://www.fmcsa.dot.gov/hours-service/elds/implementation-timeline**.

[9] *Id.*

[10] *Are AOBRD Devices Still Compliant?,* GEOTAB (Jan. 11, 2018), **https://www.geotab.com/blog/aobrd-devices**.

[11] *Here are the states that are fighting back against ELDs,* CLD Life News: Trucking News & Entertainment, (Feb. 20, 2018), **https://cdllife.com/2018/states-fighting-back-elds**.

[12] *Id.*

[13] David Cullen, *OOIDA: States Must Pass Rules Before Federal ELD Mandate is Enforced,* Heavy Duty Trucking, (Aug.29, 2017), **https://www.truckinginfo.com/141915/ooida-states-must-pass-rules-before-federal-eld-mandate-is-enforced**.

[14] James Jaillet, *New York won't issue ELD citations until state adopts rule*, Overdrive, (Jan. 7, 2019), **https://www.overdriveonline.com/new-york-wont-issue-eld-citations-until-state-adopts-rule**.

[15] Letter from Collin B. Mooney, Executive Director, Commercial Vehicle Safety Alliance, to Daphne Jefferson, Deputy Administrator, Federal Motor Carrier Safety Administration (Aug. 25, 2017) (on file with the Commercial Vehicle Safety Alliance).

[16] *Id.*

[17] Brian Straight, *Any state law undercutting ELD rule likely would violate federal regulations,* Freight Waves, (Feb. 22, 2018), **https://www.freightwaves.com/news/federal-regulation/states-seek-to-block-eld-rule**.

[18] Thomas Brewster, *How Jeep Hackers Took Over Steering and Forced Emergency Stop at High Speed,* Forbes, (Aug.2, 2016, 10:23AM), **https://www.forbes.com/sites/thomasbrewster/2016/08/02/charlie-miller-chris-valasek-jeep-hackers-steering-brake/#3a9a03163f48**.

[19] Susan Carpenter, *Cybersecurity Experts: Autonomous Trucks are Ripe for Hacking, Ransom,* Trucks.com, (Dec. 5, 2017), **https://www.trucks.com/2017/12/05/cybersecurity-autonomous-trucks-ripe-hacking**.

[20] David Goldman, *Chrysler recalls 1.4 million hackable cars,* CNN Business, (July 24, 2015, 4:29PM), **https://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html**.

[21] The SAE J1939 is a high-level protocol standard that defines communications between nodes in particular equipment. It was developed by the Society for Automotive Engineers as the preferred control access network for on and off-highway vehicles. See *Q&A–What is SAE J1939?* Axiomatic: Global Electronic Solutions, (July 6, 2006), **http://www.axiomatic.com/whatissaej1939.pdf**.

[22] Heavy Vehicle Cyber Security Update from National Motor Freight Traffic Association, Inc. (Aug. 2017) (on file with National Motor Freight Traffic Association, Inc.).