MARSH & McLENNAN AGENCY

APRIL 2018

ELECTRONIC LOGGING DEVICES

A HACKER'S NEW WINDOW TO YOUR WORLD?

By Michael C. Glover and Bryan R. Feldhaus Lommen Abdo P.A., Minneapolis

Electronic Logging Devices ("ELD") are now required for drivers of many commercial motor vehicles ("CMV") in the United States. ELDs are the electronic equivalent of a paper log used to record a driver's working and driving time.

The new mandate will result in hundreds of thousands of new internet connected devices and opens another opportunity for hackers to access, expose or destroy critical private or personal information. Hackers can severely disrupt or wholly-disable a motor carrier's operations if not handled properly.

Wise drivers and motor carriers realizes that each ELD poses a security threat *potential* not only to that truck and that driver, but all the things that it directly or indirectly connects to. That includes the truck itself and, if not properly configured and secured, the entire outside electronic world. A modern day truck's wired and wireless electronic systems connect to each other, the ELD, to the manufacturer and, quite often, to the motor carrier. The ELD itself connects to the truck, the motor carrier via cell or wi-fi and to, again at times, law enforcement via USB, Bluetooth, or e-mail. In addition, the ELD might connect to the driver's own devices, which is, in turn, connected to the internet and its many hazards.

Wise drivers and motor carriers realizes that each ELD poses a security threat potential not only to that truck and that driver, but all the things that it directly or indirectly connects to.

An ELD is, directly and indirectly, a new member of the so called internet of things ("IoT"). The best description of an IoT device is something that formerly stood alone, like your home thermostat, which now connects to other things through the internet. Those other things can be good, like connecting to your smartphone so you can turn up the temperature before you get home. Or those other things can be bad, like a hacker using the thermostat as an access point to your home computer network. The same holds true for ELDs. If not properly installed, configured and maintained, ELDs, to hackers, are as enticing as a logging in to the motor carrier's networks.

From a motor carrier's perspective, each ELD is another potential access point to company critical information and, perhaps worse yet, access to create company-wide havoc. ELDs contain "on board" information such as identifying personal information about the driver and her whereabouts. They may also contain less obvious information about the truck, the trailer, the refrigeration unit or the cargo. Depending on how they are integrated into other information systems, an ELD may contain, or have direct access to, back office information about company routes, communications, customers, dispatching, billing and costs. Not considering all of these risks subjects company information and private employee data to exposure, damage, and manipulation by hackers.

Carriers must give substantial attention to electronic security when purchasing, installing, securing and maintaining an ELD. Unfortunately, recent cyber-attacks have confirmed that no computer or digital device is completely secure. But motor carriers must take certain steps in the ELD implementation process to minimize the risk of cyber intrusions. Many of these suggestions are offshoots of electronic network and computer "best practices" utilized for office computer and phone networks. Carefully applied, these steps can minimize, but not eliminate, all risks.

SECURITY STEPS TO CONSIDER

At the equipment evaluation stage, motor carriers should only work with trusted vendors possessing proven reputations Consider engaging a consultant with experience in the industry. Obviously, carriers should only consider devices registered with the Federal Motor Carrier Safety Administration ("FMCSA"). Carriers should also give strong consideration whether the ELD should allow any interaction with a driver's personal device through any means (wired, wireless or Bluetooth). Many experts say "no" because of the sensitive data those devices may contain and the sometimes woeful security procedures people generally employ on their personal devices. Further, carriers should consult with vehicle manufacturers to better understand what risks may be associated with that type of vehicle and an ELD.

Additionally, carriers should consider whether the device should use wi-fi or bluetooth connections beyond the limited possible communication with law enforcement. This is a particular concern for ELD's using internal wi-fi or bluetooth capabilities to connect to a smartphone, tablet or laptop. Without robust security protecting that wi-fi or bluetooth network, the ELD may be susceptible to outside hackers. In fact, some experts do not recommend using bluetooth for an ELD other than to transmit carefully limited information to law enforcement. A wired connection between the dedicated input device and the driver is generally the most secure. Communication beyond the truck and law enforcement, over unsecured wi-fi should be avoided. Open wi-fi networks can be notoriously unsecure and, therefore, experts recommend using only cell phone carrier data connections for communications beyond the truck's cab. Almost no "free public wi-fi" is ever well-protected and, what's worse, such networks may be constructed simply to bait unsuspecting users for the purpose of hacking.

Without robust security protecting the wi-fi or bluetooth network, the ELD may be susceptible to outside hackers.

PURCHASING

When purchasing ELD equipment, carriers should carefully review the equipment warranty information to determine if it includes warranties about the ELD software's security, in addition to day-to-day functionality. Vendors should guaranty their hardware and software should be listed with the FMCSA registry of compliant ELDs for the duration of the device's life. Carriers should also demand a specific remedy from the vendor if the ELD is "de-registered". But remember that the FMCSA rules focus on data integrity and driver privacy, not security. Thus, carrier should not assume that an ELD registration with the FMCSA provides any data security.

INSTALLING AN ELD

ELDs should be professionally installed. Particular attention should be paid to the physical connection between the ELD and truck, which connection can be easily hacked by someone with the briefest of access to a truck. The connection between an ELD and the truck should be secure and designed to indicate whether it's been compromised. Additionally, all software utilized to maintain the connection between the ELD and the truck should be current and should be routinely updated. Occasionally, between the ELD's assembly date and its vehicle installation date, the ELD vendor might issue several software updates that contain important security patches that will not be applied unless the software is updated.

MARSH & McLENNAN AGENCY

After the initial ELD installation and programming, any remote software diagnostic access to the equipment should be closed or disabled, including access by the manufacturer. It can be opened later, if necessary. Manufacturer assigned default passwords for users and administrators must also be changed. Multiple failed logins should force a device lockdown necessitating an administrator reauthorization process. However, give thought to that process if it occurs to a driver at 2:00 a.m. as the reauthorization process can be completed remotely using appropriate authentication protocols.

TRAINING ON ELD USE

Carriers should educate drivers about the importance of proper security when using their ELD. Drivers should memorize their login and password information instead of placing post-it notes on the ELD screen. Logins must be, by FMCSA rule, unique to each driver. Also, to maximize security, passwords should have a raised level of complexity in length and content by requiring the use of numbers, capital letters, and special characters. Carriers should force password changes periodically and prohibit the re-use of old passwords. Experts suggest using a two-step verification process for login to enhance security. Consider adding another item to a driver's daily or pre-trip inspection checklist to be sure the ELD and its connections are free from any evidence of tampering. Develop a procedure for the driver to follow if anything about the ELD is out of place or doesn't "look right".

DAY-TO-DAY USE

First, keep the software current. Vendors should provide frequent and easy software and firmware updates without charge. Those updates can protect ELDs from later discovered security concerns as well as offer feature enhancements. Carriers should also develop a process to regularly install software and security updates for all aspects the ELD's operation and make vendors demonstrate the secure update process. Be sure that process does not leave administrator level access wide open between updates. Second, keep back office software similarly up to date. Third, strongly consider using professionally managed offsite storage and back up of all ELD data. Like using well known cell phone networks, well known data storage and hosting services provide increased security and physical separation for stored ELD data.

Again, in the back office, consider whether to connect the ELD network with other business-related computer networks (such as accounting, customer or vendor access) or not. Depending on the ELDs integration into any other in-cab communication capable devices, it may be wise to have no connection between the ELD network and anything else at all. This physical separation may significantly protect the motor carrier's other networks from hacks coming through the on-road ELDs.

Overall, ELDs demand additional security vigilance which must mesh with a well-designed scheme most motor carriers already have in place. However, if a company's existing security measures are woefully inadequate, the installation of ELD's may be just the incentive needed to adopt an enterprise wide data security plan. Don't think that tens, hundreds or thousands of new ELDs used by only-newly trained drivers and back office staff do not increase hacking risks. They do.

TALK WITH MARSH & MCLENNAN

If you have any questions regarding security concerns in the trucking industry, please contact Mike Glover at 612.336.1269 or Bryan Feldhaus at 612.336.4389 at Lommen Abdo, P.A., Minneapolis (general 612.339.8131). Or contact your local Marsh & McLennan Agency representative for assistance.