PEOPLENET
A TRIMBLE COMPANY

CONNECTED TRUCK SECURITY: SLAMMING THE DOOR ON HACKERS

This white paper provides an overview of cybersecurity for connected fleets and outlines frequently-asked questions and answers about data security, wireless vulnerabilities and considerations for carriers seeking the most secure fleet management technology.

The Current Situation

The Internet of Things (IoT) has become a favorite target for cyber-criminals in recent years, but the forthcoming electronic logging device (ELD) mandate has created a new sense of urgency for fleets concerned about cybersecurity. A 2016 AT&T report on security threats revealed a 3,198-percent increase in the number of attackers scanning for IoT vulnerabilities during the past three years, a number that will almost certainly increase as the number of connected devices grows.

While high-profile hacks of connected consumer electronics – such as smart televisions, climate control systems and home computers – occasionally make the news, data security is of particular concern to the trucking industry, where more than three million electronic logging devices (ELDs) are slated for deployment before the federally-mandated December 18, 2017 deadline. The connectivity of ELDs – using a cellular data network to share critical data ¬– raises considerable concern about cybersecurity.

The Cost of Being Unprepared

The risks associated with being hacked aren't unique to the trucking industry, but the potential for catastrophic financial and operational damage is elevated in an industry that moves $4 billion worth of freight each day. Any service interruption that leaves trucks idle and loads undelivered has the potential to shut down an entire business, an expensive proposition that may alienate customers and force them to a competitor. Furthermore, any loss or compromise of sensitive data – especially shipper data – can have serious business repercussions, further damaging trust and credibility between a carrier and its customers.

Consider, for example, a Texas-based long-haul fleet that in 2015 was targeted by hackers in a ransomware attack. The hack started out as an innocent-looking email purporting to be from a truck driver seeking employment. However, the message contained malicious software that quickly replicated on the company's main server and locked out authorized users before demanding a ransom payment in exchange for relinquishing control of the server. Even more troubling was the revelation that hackers had stolen all of the company's customer data and reached out to freight brokers under false pretenses, booking loads and insisting on advance payment in cash. In addition to the monetary losses the company incurred, the company suffered from immeasurable reputational damage.

This case example illustrates the high cost of inaction when it comes to cybercrime; an average of $12.7 million in losses across all industries, according to one study by the Ponemon Institute. Yet, the most significant damage often comes from the reputational fallout. If a carrier is entrusted with sensitive information – about load values, truck locations or any other details that could be exploited by criminals – and that trust is breached, the potential for damage to the customer relationship is extremely high.

Identifying and eliminating vulnerabilities

Since mobile cybersecurity is such a high priority for both carriers and technology companies serving the trucking telematics market, it's essential for industry leaders to develop solutions that address and eliminate the risks associated with this emerging threat to connected fleets. As one of the largest fleet mobility providers, PeopleNet has taken an active leadership role in cybersecurity, focused on eliminating and protecting against threats before they occur.

Among the most common vulnerabilities connected fleets face:

Service interruptions
which can occur when hackers disable key systems through distributed denial-of-service (DDOS) attacks. These attacks have the power to slow or stop freight traffic, potentially causing millions of dollars in delays and impacting everything from truck routing, shipper bills and invoices and driver payment.

Data breaches
which can adversely impact everything from mandated record-keeping to sensitive personal and business information, such as social security numbers, tax identification numbers, real-time locations for equipment and high-value freight and customer information that can be exploited by competitors.

On-board computer hacks
which exploit hardware vulnerabilities (usually through physical access to the truck) to spoof diagnostics, redirect or cancel vehicle alerts, disable critical on-board systems or even seize control of a truck's powertrain, with potentially devastating results.

While wireless hacking is often perceived as a vulnerability, there are no reported instances of trucks or telematics systems being hacked remotely. Technology leaders like PeopleNet build multiple layers of security into software architecture and hardware devices, preventing hackers from breaking through and accessing the truck or system. PeopleNet also partners with the largest cybersecurity leaders in the U.S. to uncover new vulnerabilities and institute progressive security improvements to ensure that wireless hacking remains a non-existent threat.

Understanding fleet technologies

Before examining preventative anti-hacking measures, it's essential to understand how in-cab technologies work.

One of the most basic functions of a fleet telematics solution is vehicle tracking, using GPS or cellular triangulation to determine vehicle location, speed and direction. Data is then transmitted via satellite so fleet managers can see real-time locations and quickly respond to any events in the field without communicating directly with drivers or customers.

Another important function for fleet management systems is remote diagnostics, allowing fleet managers to connect to a vehicle's onboard computer – typically through an electronic control unit (ECU) and vehicle bus and gather critical system data, such as mileage, fuel consumption and driver behavior. The data can then be used to ensure that both fleets and drivers are meeting key performance indicators, improving efficiency and profitability.

Electronic logging devices (ELDs) are perhaps the most recognized on-board technology for truckers, transforming paper record-keeping in order to track hours-of-service, roadside inspections, compliance metrics and safety goals digitally and in real-time.

Encryption and data obfuscation are two of the most effective ways PeopleNet is implementing cybersecurity measures throughout its platform and devices. These two measures ensure data is transmitted in a binary format and sent separately from the encryption keys, so there is no way to decipher what the data shows even if it isn't encrypted. PeopleNet's multiple layers of security eliminate the risk of hacking, providing peace of mind that electronic logs, the truck engine, brakes, etc., cannot be accessed remotely through PeopleNet's in-cab devices or system.

Security is also a key priority at the network layer and the application layer, with custom server and network configurations, as well as active controls like an intrusion prevention system (IPS) that actively monitors all data in the system and looks for patterns that reveal potentially damaging viruses and data breaches. The PeopleNet IPS is not a passive control; the system actively searches out and targets any incursions, while monitoring data access and other administrative actions that could serve as points of vulnerability.

PeopleNet also recently debuted the PeopleNet Connected Gateway (PCG). The PCG was built with security in mind, with additional layers of protection to further strengthen the company's hardware security. The new hardware connects to the engine bus and delivers secure cellular satellite communication back to the data center, where it is further protected with authentication and encryption protocols.

Security is part of every PeopleNet product design from the beginning, in order to benefit the entire mobility industry. The company understands implicitly the value of customer data and goes to great lengths to protect that data from hackers, a benefit that sets PeopleNet apart.

How to Choose Technology with Security in Mind

PeopleNet has taken a proactive stance on security in the trucking technology marketplace, rather than waiting to react to market needs. This commitment is the foundation for the PeopleNet ConnectedFleet™ Platform, a comprehensive fleet mobility solution that integrates pure SaaS and mobile technologies with real-time predictive analytics. Launched in 2015, ConnectedFleet is designed to share shipper data with all facets of the supply chain securely, exposing relevant data using application programming interfaces (APIs) tailored to each customer's need.

The company's cyber-sharing program joins the broader cybersecurity community together with technology providers and agencies that help look for vulnerabilities through "ethical hacking" and best-practice education. PeopleNet's security experts are also active members of the National Highway Traffic Safety Administration (NHTSA), National Motor Freight Traffic Association (NMFTA) and the CyberSecurity Alliance. PeopleNet also participated in the 2017 CyberTruck Challenge to advance cybersecurity knowledge throughout the fleet telematics industry.

As technology evolves, cybersecurity is going to continue to be a primary concern for the industry. Computers are already performing more essential functions on vehicles, which elevates risk and vulnerability. But the mere fact that security is more top-of-mind for fleet managers, manufacturers and drivers means that there is a bigger appetite for education, a silver lining to an otherwise troubling trend.

Additional features of the PeopleNet cybersecurity program include:

- Personally Identifiable Information (PII)-compliant electronic log solutions
- ISO 2013 certification
- Embedded authentication chips in in-cab devices
- Frequent security audits and software/hardware improvements
- Productive partnerships with truck original equipment manufacturers (OEMs) to minimize cybersecurity risks
- Data-sharing restrictions that prevent other applications or vehicles from receiving sensitive information
- Secure HTTP (SSL/TLS) protocols, similar to what financial institutions use to protect data
- A single, centralized point of control for all wireless communications
- Passive and active controls to detect and prevent security breaches
- Meets or exceeds Enterprise Mobility Management (EMM) standards for security

PeopleNet's ongoing commitment to continuous improvement in cyber-defense helps ensure fleets and the entire industry have the skills and knowledge necessary to prevent potential cyberattacks and eliminate the threat of exposure. As a top priority for both carriers and manufacturers, PeopleNet is taking an industry-leading role in developing solutions that leverage the best of cybersecurity principles and best practices for the trucking industry.

About PeopleNet

PeopleNet provides solutions to help fleets improve safety and compliance and reduce costs. PeopleNet's network communications, mobility and analytics products are used by more than 2,000 truckload, LTL, private, and energy services fleets throughout North America. PeopleNet was established in 1994 and is headquartered in Minnetonka, Minnesota, with an office in Ontario, Canada. PeopleNet is a Trimble (NASDAQ: TRMB) Company and part of its international Transportation and Logistics Division.

To learn more about PeopleNet and its products, visit www.peoplenetonline.com or call (888) 346-3486.

Key Takeaways:

Cybersecurity is a growing concern for the trucking industry, where more than three million electronic logging devices (ELDs) are slated for deployment.

$4 billion

The potential for catastrophic financial and operational damage due to a cyber-attack is elevated in an industry that moves $4 billion worth of freight each day. Any service interruption that leaves trucks idle and loads undelivered has the potential to damage trust and credibility, and even shut down an entire business.

That's why it's important now more than ever to work with a technology partner committed to protecting your fleet against cybersecurity. When evaluating technology providers, include cybersecurity criteria in your selection process.

Key Statistics:

A 2016 AT&T report on security threats revealed a 3,198-percent increase in the number of attackers scanning for IoT vulnerabilities during the past three years.

More than three million electronic logging devices (ELDs) are slated for deployment before the federally-mandated December 18, 2017 deadline.

$12.7 million

Cybercrime results in an average of $12.7 million in losses across all industries, according to a study by the Ponemon Institute.

Key Security Measures:

Active controls like an intrusion prevention system (IPS) add an extra layer of protection for sensitive data.

Personally Identifiable Information (PII)-compliant electronic logs ensure personal and business information is completely secure.

Encryption and data obfuscation make certain that encryption keys and data are always separate.