White Paper:

Cybersecurity and the Trucking Industry

GTG Technology Group

GTG Technology Group, LLC builds software to manage global transportation management systems (TMS) for all sizes of intermodal brokerage, and drayage transportation companies. GTG is dedicated to providing TMS solutions designed to provide end-to-end visibility and connectivity. GTG's software is delivered as a Cloud-based Software as a Service and was engineered to help businesses in the transportation industry overcome their challenges faster, more cost effective, and more efficiently.

Contents

As Vehicles Get Smarter, Trucking Worries About Cybersecurity

Technological advancements are disrupting every aspect of the transportation industry. From the way automakers set up vehicles to the logistics software motor carriers use to manage trucking activities, most of the trucking industry features one or more internet-connected endpoints.

Technology continues to merge with everyday workflows, so companies within the trucking industry must consider the vulnerabilities each point of connectivity creates. Cybersecurity – just like regulatory compliance or human resources – is a fundamental part of business practices today.

Increased Connectivity in the Trucking Industry

Connectivity is driving the trucking industry to new heights, and autonomous vehicles are only the most obvious connection point for professionals to consider. In today's marketplace, the trucking industry already supports numerous technologically connected systems, including:

1. The connected electronic systems within each vehicle. Passenger and commercial vehicles use electronics (collectively known as the Controller Area Network) for sensing/data collection, window controls, airbag controls, the powertrain, and to control most of the displays in the dashboard. Auto manufacturers are increasingly adding connectivity features, including sensors (telemetry) and smart technologies to the internal operating systems in vehicles[1].

2. The number of telematics devices installed in U.S. trucks is expected to reach 8.1 million by 2018[2]. Real-time data transmission and system management gives support professionals an easy way to run diagnostics and efficiently maintain vehicles.

3. Software and company networking. Most organizations use logistics software to manage routing information, billing, freight exchange points, and other crucial trucking information. Many rely on cloud technology and/or a local network to run the systems from remote endpoints. While incredibly efficient and effective, these digital portals do represent a possible backdoor into company systems. Both the software and hardware used to access logistics tools can represent a vulnerability within the system.

4. Mobile devices/personal hardware. To access software and maintain communication with other professionals, truckers and support personnel may use personal or company-provided mobile devices. Mobile phones, tablets, and computers all represent points of connectivity and potential vulnerability.

While these seem like three straightforward categories, specific vulnerabilities exist within each category. For example, each new app installed on a smartphone could create a gateway into sensitive information. As augmented reality and autonomous trucks enter the marketplace, additional vulnerabilities will expand the trucking industry's threat landscape. Some estimates project that more than 50 billion devices will be connected to the internet by 2020[3].

[1] http://www.supplychain247.com/article/how_the_internet_of_things_transforms_trucking/webcasts
[2] https://www.trucks.com/2016/05/17/long-haul-trucking-connectivity-brings-hacking-risks/
[3] http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf

The Modern Cyber Threat Landscape

To put the realities of cybersecurity into perspective, consider the realities of a security breach. According to a security report, the average cost of data breaches are rising. Today, a data breach costs organizations an average of $4 million[4]. Depending on the type of organization, the sensitivity of information, and the number of records compromised, the average cost per record is $158.

The Identity Theft Resource Center tracks the number of data breaches that occur every year. In 2015, the organization counted 781 total attacks[5]. The business sector faced the highest number of breaches followed by the health and medical sector. While information may be valuable in these industries, cybercriminals may have different goals when they hack into transportation company systems – to remotely disrupt and control transportation systems.

In September 2016, global advisory and risk management group, Willis Towers Watson, released a Transportation Risk Index 2016: Navigating risk in the transportation sector[6]. The organization looked at the 50 risks and five megatrends reported by 350 senior executives in the industry. Their findings shed light on the unique cybersecurity concerns faced by the transportation industry:

1. Cyber vulnerability is the single most significant threat faced by the transportation sector.
2. In the land transportation sector, executives are most concerned about third-party logistics vulnerabilities.
3. The threats transportation companies face today are very different from past threats.
4. All top threat trends including cyber vulnerability, regulatory uncertainty, a changing market, talent management difficulties, and stability within globalized operating models are interconnected.

To address the threats facing transportation (and any other industry) today, companies must consider the technology they use, the people who use it, and market changes. Failing to address cybersecurity concerns may not jeopardize an entire operation today or tomorrow, but companies must change their approach from an “if it happens” to a “when it happens” mentality.

[4] https://www-03.ibm.com/security/data-breach/
[5] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html
[6] https://www.willistowerswatson.com/en/insights/2016/09/transportation-risk-index-2016

Examples of Security Risks in the Automotive Industry

Security risks in the automotive industry have already affected those within the transportation industry. Here are some real-world examples that showcase the impact of a cyber threat:

- Security researchers remotely take over a big rig[7]. In 2016, after tests proving the vulnerability of Jeep Cherokee and Chevy Impala internet connected systems, cybersecurity researchers turned their attention to tractor trailers. The researchers were able to manipulate the systems within a 2006 tractor-trailer and a 2001 model school bus using a remote laptop keyboard.

For the test on the big rig, the white-hat hackers were able to spoof the readings on the gas gauge, prevent the driver from seeing accurate compressed air readings for the brakes, and remotely disable the braking system, among other things. Since most industrial trucks feature standardized systems, hackers could access numerous vehicles using one attack.

- TL carrier OutWest Express' main server hacked. In 2015, this long-haul trucking company from Texas experienced the ramifications of a cyberattack firsthand when hackers tapped into the company's main server[8]. Cybercriminals used a feigned driver application résumé attachment in an email to infect the server with ransomware. The criminals changed all server logins and made their demands. The thieves not only held the company's information for ransom, they used it to steal from freight brokers.

The company was not prepared with adequate backup data stores and it never recovered all the data lost in the breach. The example highlights the importance of proactive prevention, as well as an effective reaction.

- Physical theft assisted by cybersecurity breach. In California in late 2015, a shipment containing 45,000 pounds of shelled pistachios (worth about $450,000) was stolen right from under the grower's nose[9]. In this case, the thieves were part of a high-tech group that hacked databases in order to gain legitimate information and fraudulently drive away with a truckload of nuts.

On the day of the shipment, the paperwork was messy, but nothing seemed out of place. When the growers caught on to the theft a few hours later, the truck had already been unloaded and abandoned.

- Security researcher finds vulnerable telematics systems. Another security researcher was able to discover thousands of telematics systems using a specialized search engine online[10]. The researcher was able to both monitor and control vehicles after gaining access to the system.

These examples showcase the range of threats faced by the trucking industry today. Cybercriminals are getting smarter and looking for new ways to access information, systems, and freight.

[7] https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/
[8] http://fleetowner.com/technology/battling-hack-one-fleet-s-story
[9] http://www.latimes.com/business/la-fi-nut-theft-20160414-story.html
[10] https://www.trucks.com/2016/05/17/long-haul-trucking-connectivity-brings-hacking-risks/

Who is Responsible for Maintaining Cybersecurity in the Trucking Industry?

Cybersecurity requires the involvement of everyone who comes into contact with a piece of technology. In the trucking industry, motor carriers, logistics organizations, IT departments, support personnel, truckers, third-party vendors, and auto manufacturers all play roles in maintaining cybersecurity within an organization.

Although many people play a role in maintaining cybersecurity, some individuals face more responsibility for threat prevention and response activities. For cybersecurity policies to work, organizations must take a top-down approach. With executive management on board, companies can create plans to minimize the risks associated with interconnectivity in the modern trucking industry.

Identifying Vulnerabilities in Your Trucking Business

Cyber vulnerabilities come in many shapes and sizes. The first step in effectively addressing cybersecurity within an organization involves conducting a security audit of the following factors:

- People. Businesses must consider people within the organization as they evaluate their security vulnerabilities. Many cyber threats arise from employee ignorance, carelessness, or malicious intent. In some cases, millennial employees could pose the most significant threat[11]. People who are unafraid of using technology and use it without thinking about the repercussions can unwittingly expose the entire network to a malware attack.

- Processes. While people control connected end points, companies are responsible for creating formalized processes for preventing and addressing cyber threats[12]. Trucking organizations must constantly research new threats, test existing systems, and create plans of action that all employees can use to appropriately act and react to potential threats.

- Data. Aside from employees, data is one of the most valuable assets a company holds. When a criminal hacks into data on payment and billing information, routing, security protocols, contact information, and other sensitive information, companies and anyone they manage data for lose. Employees, clients, and others may all suffer if a cybercriminal steals information. Data privacy and security plays an integral role in any cybersecurity management program.

- Hardware. Physical devices, including personal and company-owned devices, servers/networking, and IoT devices all play roles in cybersecurity. Companies need to create clear instructions for when, how, and where employees use hardware. Accessing a routing management system using the local coffee shop's Wi-Fi connection represents a vulnerability.

These four main categories deserve attention on a regular basis. An audit of each area will yield valuable information about an organization's current state of cybersecurity. From there, companies can create and/or optimize their prevention and response policies to reduce the overall levels of risk.

[11] http://fortune.com/2016/06/15/millennial-employees-cybersecurity-risk/
[12] http://www.nationalcybersecurityinstitute.org/awareness-month-2015/podcasts-awareness-month-2015/people-process-and-technology-national-cybersecurity-awareness-months-1st-podcast/

Developing a Cybersecurity Policy

With a comprehensive audit in hand, any organization can create an effective cybersecurity policy. Regardless of the industry, security policies/strategies define terms, outline processes, and create chains of command for both preventative and reactive cybersecurity practices.

Every policy will vary based on the company, its technology, and its individual challenges, but a strong cybersecurity policy may include the following elements:

1. Data privacy and security terms. All data is not created equal. Some data should remain private while general data and public data may not represent a threat to the organization. A cybersecurity policy should outline the parameters for each security level, and create processes surrounding data handling and privacy. Whether an organization works with cloud data storage companies or uses its own servers for management, comprehensive backup processes, access rights, and storage parameters can reduce the risk of data privacy threats.

2. Vulnerability scanning and testing process outlines. Companies may not need to undergo comprehensive audits on a regular basis, but small and large companies do need to scan systems regularly for vulnerabilities. Consider placing different systems and digital assets on a rotating schedule. Scan and test each one throughout the year to maintain strong security protection at all times. The cybersecurity policy should outline when scans take place and the response process for identified threats.

3. Patch management. Patch management allows organizations to manage existing vulnerabilities in an efficient way. Code patches address potential vulnerabilities and can strengthen the overall security of the system[13]. Within the cybersecurity policy, a patch management section should discuss when and how the company addresses patch management activities. Patch management is such a significant part of cybersecurity practices that many security vendors including IBM and Kaseya VSA now offer automated patch management programs.

4. Network security configurations. The IT department is on the front lines of cybersecurity and threat management. Work with IT specialists to develop a set of network security guidelines to outline the rules for server management, antivirus practices, firewall management, account management, and other network-related activities. These security activities also may involve enhancing the usability of secured applications.

5. Incident response plans. What happens if and when your IT department detects a security breach? An incident response plan will cover the exact steps key personnel take when an organization identifies a significant threat or a breach.

[13] http://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy

A cybersecurity incident response plan may include a list of incident response team members, lockdown procedures, impact minimization techniques, and steps for preventing similar threats in the future[14]. Most policy content may remain the same for years, but the incident response plan may change. Refresh your plan regularly to keep up with organizational changes and the ever-changing threat landscape.

6. Employee guidelines. Every employee should understand his or her role in cybersecurity management. These guidelines should remind management of organizational training policies regarding cybersecurity and help employees understand their individual responsibilities. Education and training play integral roles in threat management.

   Employee guidelines may specifically outline website, email, and mobile device usage, and may feature an incident-response report employees can use to report threats to management[15]. Consider implementing employee cybersecurity training as part of new hire orientation and develop an annual program to remind existing employees about company policies and new threats. Whether an organization supports 15 employees or 1,500, employee cybersecurity practices can protect individuals and organizations from the consequences of a security breach.

7. Third-party collaboration. Many organizations partner with third parties for logistics, transportation management, payments, and other activities. Third parties may or may not employ strong data privacy and/or security protocols, which could put a client's organization at risk. While it is in a third party's best interest to maintain a strong reputation for security and privacy, formalize the communication process for current and future activities. A transparent and collaborative relationship with third parties will enhance the privacy for both organizations[16].

8. Asset acquisition policies. Acquiring new technology can leave gaps in any cybersecurity policy. To avoid creating vulnerabilities during the acquisition process, create guidelines individual departments can use to request funding, conduct research, and acquire new solutions. When departments work closely with IT and security professionals, the organization can minimize the risk associated with shadow IT (when departments and individuals invest in or use technology solutions that the IT department does not support and/or the organization does not sanction).

9. Regulatory compliance. While the federal government does not enforce many direct cybersecurity-related rules on the trucking industry, rules for increasingly connected trucks are just around the corner. Consider compliance from a data privacy and technology point of view to protect company information and comply with any existing and new regulations as they affect the industry.

[14] http://www.csoonline.com/article/3104203/techology-business/4-steps-to-a-strong-incident-response-plan.html
[15] https://www.dhs.gov/sites/default/files/publications/FCC Cybersecurity Planning Guide_1.pdf
[16] http://www.prnewswire.com/news-releases/automotive-industry-collaborates-in-developing-vehicle-cybersecurity-best-practices-to-address-cybersecurity-challenges-300301805.html

Strong cybersecurity in the trucking industry requires transparency, collaboration, and formalization. Since trucking involves many moving parts, each organization must look at its own role in the supply chain and protect every endpoint that may represent a vulnerability.

The Future of Cybersecurity and Trucking

The health care, financial, and government sectors already face heavy federal regulations regarding cybersecurity. As other industries use connected technologies more often, they may begin to see changes in their own regulatory landscapes. The National Highway Traffic Safety Administration (NHTSA) is already moving for more rules regarding the security of automotive control systems[17]. As passenger vehicles and commercial trucks become smarter and more connected, cybersecurity will become an integral part of the trucking business.

In 2015, the trucking industry earned $726.4 billion[18]. People and businesses rely on safe and affordable freight transportation on a daily basis. Trucking companies including Daimler's Mercedes-Benz are working hard to make autonomous tractor-trailers a reality. Uber-owned company, Otto, is developing augmented driving systems existing trucks may one day use. The industry is advancing at a rapid rate, and driver support and technology are playing increasingly important roles. As technology integrates more within the industry, motor-vehicle carriers and trucking-related organizations must consider the reality of cyber threats.

Investing in adequate cybersecurity preventative maintenance and response solutions could save small and large trucking companies from suffering major losses. Paying now will likely result in a better economic outlook than trying to afford the costs associated with an attack later.

[17] http://www.autonews.com/article/20160119/OEM06/160119727/nhtsa-chief-vows-action-this-year-on-cybersecurity
[18] http://www.trucking.org/article/ATA-American-Trucking-Trends-2016

Notes