TRANSPORTATION INSIGHTS

LloydSadd INSURANCE BROKERS

NAVACORD®

Cyber Risks in the Transportation Industry

Not only are cyber attacks increasing in size and severity, they are now affecting industries that were once relatively safe. This is especially true for the transportation and trucking sectors, as the adoption of new technologies has opened new doors for hackers.

In fact, just one cyber incident can put a trucking company's vehicles, data and employees at risk. In order to protect your fleet, employees, customers and bottom line, it's important to understand the common cyber risks in the transportation industry.

NEW TECHNOLOGY VULNERABILITIES

With the advent of telematics and embedded software, trucks are more connected than ever before. While this connectivity can simplify data collection, increase efficiency, reduce costs and improve safety, it also increases the likelihood that a fleet will be targeted by a cyber criminal.

In just a few minutes, hackers can steal the private data your fleets collect. This data can then be ransomed against your firm. In addition, vehicles with embedded software can be accessed and taken control of by malicious parties, putting the safety of your drivers and the general public at risk.

Vehicles with embedded software can be accessed and taken control of by malicious parties, putting the safety of your drivers and the general public at risk.

CARGO THEFT

Cargo theft is a chief concern for fleet managers, and new technology creates vulnerabilities that make it easier for criminals to steal freight.

Through a tactic known as "fictitious pickup," thieves can easily look up the routes of valuable loads. Then, using fraudulent credentials, they can access a contract, arrive at the listed pickup point, load up the cargo and drive away, all without being detected. This deception can be incredibly costly and damage a fleet's bottom line, productivity and reputation.

In addition to implementing the fictitious pickup scheme, criminals can steal cargo by hacking a truck's telematics system and disabling its acceleration and brakes. After disabling the vehicle, the criminals could easy overtake the driver and take off with the freight. Using a similar strategy, criminals could hack a truck and strand the driver, suspending product delivery until a ransom is paid.

LOSS OF PERSONAL DATA

- Any organization that stores or transmits sensitive data can become the victim of a cyber attack. For firms operating in the transportation industry, information at risk includes, but is not limited to, the following:
- Sensitive employee or customer data, including credit card numbers, addresses and birthdays
- Sensitive information from vendors, providers and other partners
- Any proprietary or intellectual property you store
- Logistics, freight, billing and collection data

Theft of any of the above information can financially sink a company or take away its competitive advantage. In some cases, loss of sensitive data can enable competitors to steal processes, systems, concepts or designs.

Just one cyber incident can put a trucking company's vehicles, data and employees at risk. In order to protect your fleet, employees, customers and bottom line, it's important to understand the common cyber risks in the transportation industry.

SOCIAL ENGINEERING

Social engineering is the act of taking advantage of human behaviour to commit a crime. Social engineers can gain access to buildings, computer systems and data simply by exploiting the weakest link in a security system—humans. For example, social engineers could steal sensitive documents or place key loggers on employees' computers —all while posing as fire inspectors from the nearby fire department.
Social engineers don't need to have expert knowledge of a company's computer network to break in to a business—all it takes is for one employee to give out a password or allow the engineers access to an area they shouldn't be in.

OTHER COMMON EXPOSURES

Cyber attacks can expose companies to a wide array of liabilities. Some of the most common claims relate to:

Data breaches: If a criminal manages to steal a company laptop or hack into an IT system, they may be able to access sensitive information about your clients, like financial data or personal health information.

Cyber extortion: From the other side of the World, hacker can enter an IT system and prevent a company from accessing its own data until a ransom is paid

Intellectual property rights: Including libel, copyright or trademark Infringement, and defamation stemming from a company's online activities.

CUSTOMIZE YOUR PROTECTION WITH CYBER INSURANCE

As the transportation industry becomes increasingly connected, a wider range of data will be transmitted across networks. While storing data is a necessity for modern businesses, trucking firms will need to take the proper precautions in order to protect sensitive information, their fleet and customers.

The best way to protect your fleet from cyber criminals is through cyber insurance. These policies can be tailored to meet the unique needs of your firm, ensuring that you are ready if and when an attack occurs.

If you have questions specific to cyber protection, or would like additional information, please reach out to your local advisor.

LET US HELP YOU MANAGE YOUR RISK

LOCATIONS
Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330

lloydsadd.com
navacord.com
info@lloydsadd.com