AMWINS

Top 8 Cyber Risks Facing the Transportation and Logistics Industry

Every industry group has exposure to cyber risks, including transportation and logistics. Like other industries, the days of paper and land lines have transitioned to networks, digital devices, applications, and web-based tools that are critical to operating in this industry.

Below are the top eight cyber risks insureds are currently facing in the transportation and logistics sector.

1. Social engineering

Companies often pay bills electronically as well as confirm payment details through the exchange of emails. Any online transactions are susceptible to a social engineering loss. Even if criminals do not enter a firm's computer network, they can craft what appears to be a legitimate email message from an authorized officer of the company directing the accounts payable department to wire funds to a criminal's account. The criminal may monitor social media to see when that authorized officer is out of the office on vacation and unable to verify or stop the fraudulent instructions. According to the latest data from the FBI, thieves are making off with billions of dollars from this type of attack.

2. Hackers

Hackers are a persistent threat against all companies and individuals. Some are looking for confidential personal or business records to sell to identity thieves. Some will encrypt data or networks and hold them for ransom. Cryptocurrencies will need to be paid to get the decryption keys and retrieve the data and network access.

3. Corrupted Data

In addition to a hacker entering a computer network, authorized employees can make mistakes that destroy or corrupt data. Often, companies must engage external IT firms to restore or recreate lost data – an expensive undertaking that could be insured on a cyber policy with that type of coverage. A business interruption loss might also be incurred due to lost or corrupted data.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

4. Contingent System Failure

When a firm's clients or vendors use external computer networks to operate their businesses, there is a risk of contingent system failure. If those external networks stop, a company may not be able to receive or fulfill orders, creating a business interruption loss not covered by a property policy. When electronic files are corrupted or altered, a transportation company may not be able to fulfill its professional service of moving perishable goods from point A to B. As a result, the company may be held financially responsible for spoilage, lost shipments, and more. This is an area where professional liability and cyber liability may cross paths.

5. Inoperable Electronic Logging Devices

Many companies are subject to the ELD (electronic logging device) mandate by the Federal Motor Carrier Safety Administration. If those devices are rendered inoperable by a virus, ransomware or other hacking event, the drivers must stop driving or the organization runs the risk of being fined. In this situation, the business interruption loss arises from a cyber event.

6. Varying State Laws

Numerous state and federal privacy laws apply to all transportation and logistics businesses. The laws vary by state, and the applicable laws are determined based on where the victim resides, not where the company is based. Knowing how to respond to a privacy breach in each state requires a great deal of legal assistance, which is covered by cyber insurance.

7. Errors by Contractors

Many transportation firms do not have well-funded network security departments, so these functions are often outsourced. The outsourced experts may be highly qualified, but they can also make mistakes. An organization will still be held accountable by regulators and customers even if the network security error was committed by a contracted IT vendor or Managed Service Provider.

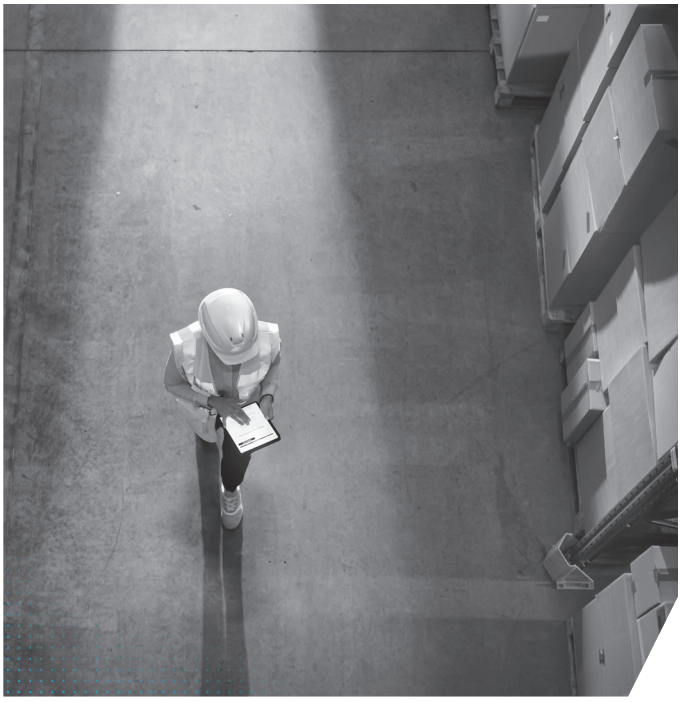
8. Bodily Injury and Property Damage

For transportation and logistics firms who deal with assets in motion, there's always a risk of bodily injury and property damage. A network intrusion could lead to numerous problems, including traffic accidents, loads exceeding weight limits, and hazardous materials being transported to an incorrect destination.

Coverages to Address the Cyber Threats Facing the Transportation and Logistics Industry

Threats targeting the transportation and logistics sector can come from:

- Criminals
- Terrorist groups
- Hacktivists
- Disgruntled or former employees
- Nation states
- Competitors
- Traditional network operation mistakes



Cyber liability policies have been designed to address many of these threats. However, this coverage is not included in other lines of business such as property, general liability, or umbrella and coverage varies by insurer.

Here are some of the insuring agreements you should expect to see in a cyber policy.

Cyber Business Interruption and Data Recovery	Covers expenses to recover from a network interruption, including lost revenue and data
Cyberextortion and Ransomware	Covers expenses for dealing with an extortion event, including paying the ransom and getting the network back online
System Failure and Dependent System Failure	Covers your lost revenue and expenses when a system you use fails, even if not triggered by a security intrusion. This can cover your system or systems provided to you by others that fail.
Network Security Liability	Covers claims against the organization when its own network is used to harm others or has been used by hackers to enter a trading partner's network
Privacy Liability	Provides coverage for first-party expenses arising from a privacy breach. Common coverage grants for services designed to reduce loss to the potential victims include notification expenses, credit monitoring, identity fraud resolution, call centers, breach coaches, IT and legal forensics, as well as public relations support to protect a firm's reputation
Regulatory Fines and Penalties	Provides coverage for defense costs and possible fines levied by a variety of different state and federal regulators arising from privacy violations
PCI Fines and Penalties	Provides coverage for claims made against the insured by a payment card company for violating PCI DSS standards related to a payment card breach
Social Engineering	Provides coverage for the insured's loss of funds after a cybercriminal tricks an employee into wiring funds to the wrong account

Cyber Risk Management Tools

In addition to reactive insurance coverage, it's also important to consider the various risk management tools available from many insurance companies. For certain accounts, some insurance companies can provide free or discounted loss prevention services, such as:

- Social Engineering spoof tests and training
- Network penetration testing
- Table-top exercises to practice preparedness with cyber attorneys
- Network traffic threat scoring
- Cyber threat information and template portals
- Free hotlines that allow network security professionals to ask configuration questions

Amwins has negotiated discounts from industry-leading vendors who provide endpoint protection and security review services that helps first time buyers and current insureds get prepared to go to market. **Learn more about these services here.**

Conclusion

The transportation and logistics sector has meaningful cyber risks that differ from other industries. A well-informed specialist broker can structure many traditional cyber insurance policies to address the industry's unique risks. Amwins has numerous specialized cyber brokers that are well-equipped and eager to assist you in placing these risks.

About the Author

This article was written by David Lewison, national Professional Lines practice leader, and Jennifer Nuest, national Transportation practice leader for Amwins.