# TOP 10 CYBER RISKS FACING THE TRANSPORTATION AND LOGISTICS INDUSTRY

## CONTACT

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

## LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

*Courtesy of AmWINS Group, Inc.*

## ABOUT THE AUTHOR

This article was written by David Lewison, national Professional Lines practice leader for AmWINS Group, Inc.

ON YOUR TEAM.

As an insurance professional, the first thing that comes to mind when you think about the transportation industry is probably not cyber liability. However, every industry has exposure to cyber risks, including transportation and logistics. While these industries worked from paper and wheels for many years, now there are both internal and external networks that are critical to operating in this industry group.

Below are the top 10 cyber risks that insureds are currently facing in the transportation and logistics sector.

1. If 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.
2. If a company pays bills to any third party, it is 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 millions of dollars from this type of attack.
3. If a network is 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.
4. Like other companies, transportation and logistics firms hold the private financial, personal and health information of their employees, as well as account numbers and other protected information of clients. A privacy risk exists even if these files are held in a paper format; this risk can be covered by a cyber policy.
5. Some 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 or the organization runs the risk of being fined. In this situation, the business interruption loss arises from a cyber event.
6. 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. 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.

*(continued on next page)*

*(continued from previous page)*

8. Allowing employees to use their own mobile devices in the workplace – to track locations, navigate, coordinate drop offs and pickups, submit bills and more – can put a company at risk. These devices can be locked with ransomware or suffer some other sort of network failure that can impact business.
9. In addition to a hacker entering a computer network, encrypting data and making extortion demands, authorized employees can make mistakes that destroy or corrupt data. Often, companies must engage external IT firms in order 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 while due to lost or corrupted data.
10. 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

However, there is coverage to help with many of these threats. The typical insuring agreements found on a Cyber Liability policy may be able to address many of these threats. This coverage is not included in other lines of business such as Property, General Liability or Umbrella. Cyber Liability coverage varies by insurer, but these 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 |
| 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 |



*(continued on next page)*

*(continued from previous page)*

## 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

## CONCLUSION

The transportation and logistics sector has meaningful cyber risks that differ from other industries. While the number of industry-specific policies are very small, 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.