

Transportation and Logistics Cyber Risk Exposures and Solutions

Cyber risk refers to the loss potential an organization faces by virtue of its reliance on information technology, connectivity and automated processes. While improved efficiency is derived from technology implementation, organizations face additional risk from the cyber exposures inherent in technology systems. In an increasingly punitive legal and regulatory environment, and in the face of more frequent contractual requirements for cyber liability insurance, forward-thinking companies are taking proactive steps to explore and transfer cyber risk.

Numerous factors contribute to an organization's cyber risk profile, including: actions by employees, system and program glitches, security measures, industry classification, nature and quantity of data collected, political or strategic significance, and reliance upon technology.

Transportation companies should be concerned about cyber risk if they:

Gather, maintain, disseminate or store private information

- Have a high degree of dependency on electronic processes or computer networks
- Are concerned about contingent bodily injury and property damage resulting from cyber incidents
- Rely on or operate critical infrastructure
- Are subject to regulatory statutes
- Are concerned about intentional acts by rogue employees
- Engage vendors, independent contractors or additional service providers

Transportation and logistics cyber concerns:

- Hackers are more sophisticated in their targeting, with tools to assist in hacking anything from a small webcam to control systems
 - Industrial control systems are typically isolated, but with newer advanced versions of operating systems and connected devices, information sharing and connectivity is a concern
- Bodily injury or property damage resulting from a cyber event

- Business / service interruption or lost income due to cyber incident
 - Hacker penetrates security and gains control of positive train control system. There is no physical damage but there are injuries to third parties occur due to blocked crossings and business interruption
- Dependent or contingent business interruption due to a cyber event suffered by a third party vendor
- Destructive malware infiltrates a company's systems (through a hack or employee clicking on a link), destroys data on the network and impacts transportation operations
- Disrupts the wireless communications / dispatching system, causing emergency braking, derailment or property damage
- Potentially large amounts of customer and employee data, depending on business operations, and costs incurred to engage legal and forensics firms, notify impacted individuals, etc.
 - Personally identifiable information risk may be less prominent in the transportation space, but remains an exposure for organizations with retail customers
- Evolving regulatory environment
- Resources allocated to physical perils rather than information and systems security

We're here to empower results

If you have any questions about your specific coverage or are interested in obtaining coverage please contact your Aon broker or visit aon.com.

The Aon acquisition of **Stroz Friedberg** enhances the ability of Aon to support clients with leading digital forensics and incident response capabilities.

Scope of cyber coverage available in the insurance marketplace

Third Party Coverage Elements

- **Security and privacy:** defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, denial of service attack or transmission of a computer virus
- **Regulatory defense and fines:** defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security
- **Media liability:** defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy
- **PCI fines and assessments:** defense costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

How do organizations transfer cyber risk?

- The cyber insurance marketplace provides service solutions, including loss control
- resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response
- Breach response coverage offering varies based on insurer and policy structure
- 60+ insurers provide cyber coverage with large capacity available

Aon Cyber Innovation

- The Aon Cyber Enterprise Solution is the first of its kind policy that broadens the scope of cyber coverage to include: property damage arising out of a network security breach, business interruption and extra expense coverage arising out of a systems failure, contingent network business interruption for IT vendors and the supply chain, cyber terrorism coverage, etc. This product provides catastrophic limit in excess of \$400M USD.

First Party Coverage Elements

- **Breach response costs associated with:** breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring / protection, notification hot-line / call center, identity theft resources
- **Network business interruption:** loss of income and extra expense due to network security failure
- **Dependent business interruption:** reimburses the insured for actual lost net income and extra expense incurred when the insured's IT service provider's computer system is interrupted / suspended due to a failure of network security
- **System failure:** coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security
- **Data restoration:** costs to restore / recreate data / software resulting from network security failure
- **Cyber extortion:** reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat

Aon Cyber Resilience Framework

- Aligned with client's risk management approach to cyber security, Aon's approach helps identify and protect your critical assets and balance sheet by aligning your cyber enterprise risk management strategy with your corporate culture and risk tolerance. To achieve this, Aon recommends the following framework:

