Aon
Cyber Solutions

Transportation & Logistics

Cyber risk exposures and solutions

Logistics companies, postal services, railways, road networks, shipping companies and ports are a target for cyber criminals with motives of financial gain via theft of confidential information or money. Cyber is a broad risk that organisations face by virtue of their reliance on information technology, connectivity and automated processes. In an increasingly punitive legal and regulatory environment, and with 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 organisation's cyber risk profile, including: action by employees, system and programme errors, security measures, industry, nature and quantity of data collected, political or strategic significance and reliance on technology.

Cyber risk considerations for transportation and logistics organisations:

- Gathering, maintaining, disseminating or storage of information
- High dependency on electronic processes or computer networks
- Potential contingent bodily injury and property damage resulting from cyber incidents
- Relying on or operating critical infrastructure
- Regulatory statutes
- Privacy regulation
- Dependence on vendors, independent contractors or additional service providers
- Higher vulnerability due to a fragmented supply chain
- Industrial control systems are typically isolated, but with advanced versions of operating systems and connected devices, information sharing and connectivity is a concern

Potential cyber incidents for transportation and logistics organisations:

- Hackers targeting Point-of-Sale systems (POS) or operation systems to gain access to the organisation's network
- Bodily injury or property damage resulting from a cyber event
- Business / service interruption or lost income due to cyber incident
- Dependent or contingent business interruption due to a cyber event suffered by a third party vendor
- Destructive malware infiltrating a company's systems potentially destroying data on the network and impacting transportation operations
- Disruption to wireless communications or dispatching system, causing emergency braking, derailment or property damage
- Security incident exposing customer and employee data resulting in legal action
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Shannan Fort
Cyber Transportation & Logistics
Insurance Industry Expert
+44 (0)20 7086 7135
shannan.fort@aon.com

Alistair Clarke
Cyber Insurance Leader
Global Broking Centre
+44 (0)20 7086 7357
alistair.clarke@aon.co.uk

David Molony
Cyber Risk Leader
Global Risk Consulting
+44 (0)777 5227008
david.molony@aon.co.uk

Spencer Lynch
Cybersecurity Leader
Stroz Friedberg
+44 (0)20 7061 2304
slynch@strozfriedberg.co.uk

Vanessa Leemans
Chief Commercial Officer
Cyber Solutions EMEA
+44 (0)20 7086 4465
vanessa.leemans@aon.co.uk

aon.com/cyber
strozfriedberg.com/resource-center

AON
Empower Results®

Scope of traditional cyber coverage available in the insurance marketplace:

Third party coverage elements

- ***Security and privacy:*** defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorised access, denial of service attack or transmission of a computer virus
- ***Regulatory defence and fines:*** defence 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:*** defence 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:*** defence costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

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 centre, 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 service provider's computer system is interrupted / suspended due to a failure of network security
- ***System failure business interruption:*** 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 has successfully negotiated the following key coverage enhancements (subject to market agreement per individual risk):

- Full limits for incident response and costs associated with breach notification
- Broad definition of computer system
- Coverage for cyber terrorism
- Deletion of the unencrypted device exclusion
- No failure to patch exclusion
- Supply chain business interruption coverage
- Cost of spoilage
- Bricking coverage – replacement costs for portions of fleet (Internet of Things)
- Delay in delivery/delay in performance coverage

Empower Results®

Our approach

Adopting a risk based cyber insurance strategy

Aon's cyber capabilities can support organisations in embracing a risk based approach through:

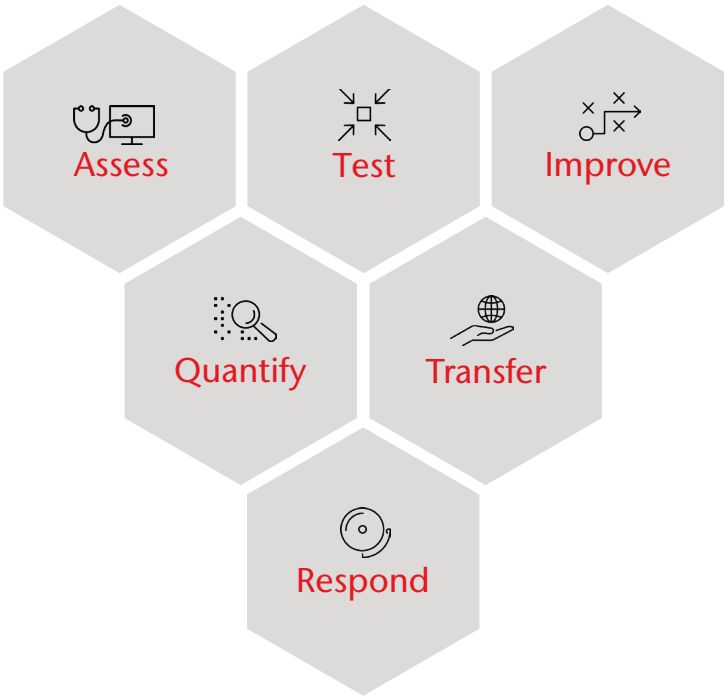
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework supporting organsations to optimise their resilience strategy through mitigation and transfer. Existing risk financing strategies can also be enhanced through modelling cyber loss scenarios and stress testing current limits.

Cyber innovation

- *Aon Cyber Enterprise Solution*™ - a policy which 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.
- *Aon's GDPR Protect Solution* - a modular risk management solution that helps organisations manage financial, regulatory and legal risks associated with processing personal data under the EU General Data Protection Regulation (GDPR).

Our cyber resilience framework

Aon and Stroz Friedberg offer a full range of services to help you approach cyber as an enterprise risk and achieve cyber resilience.



Empower Results®

Client story

Stroz Friedberg was engaged to assist a global automotive organisation with various proactive services, including security risk assessments, penetration testing, web application security testing, and incident response plan development.

The client had recently experienced some unanticipated internal organisational changes, which resulted in resource constraints, and they needed advisory assistance in continuing to drive their internal security and compliance programme during this period of change. In addition to requiring assistance in understanding and evaluating their current programme priorities, they also required advisory assistance in identifying opportunities for enhancing controls across fragmented operations.

Our cybersecurity advisory team provided assistance with ongoing security, governance, risk, and compliance efforts, in addition to assistance with preparation for upcoming internal audits related to security and controls. We helped stakeholders at several fragmented subsidiaries better understand priorities, identify opportunities for improvement and optimisation, and enabled them to focus on the areas that mattered most to the organisation. Our resources worked closely with the client's team, and were successful in enabling the organisation to meet its objectives during a period of organisational change and transition.

Our efforts were instrumental in aiding this automotive organisation's need for specialised security advisory assistance during a transitional period. Services designed to improve security and cybersecurity maturity included targeted recommendations regarding vendor management, policy governance and physical security. Our work resulted in a notable enhancement to the organisation's physical and logical security access controls and processes at headquarters and related locations.