Aon
Cyber Solutions

Industrial & Materials

Cyber risk exposures and solutions

Heavy industrial organisations like manufacturers, steel makers or mining companies 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 industrial and materials organisations:

- Gathering, maintaining, disseminating or storage of private information
- High dependency on electronic processes or computer networks
- Direct or contingent bodily injury and property damage resulting from cyber incidents
- Relying on or operating critical infrastructure
- Subject to regulatory statutes
- Dependence on vendors, independent contractors or additional service
- Network connectivity with other organisations
- Security vulnerability in connected devices and products (e.g. autonomous vehicles, Wi-Fi thermostats)

Potential cyber incidents for industrial and materials organisations:

- Hackers targeting sophisticated industrial control and data acquisition systems (SCADA)
- Dependent or contingent business interruption due to a cyber event suffered by a third party vendor or supplier
- Business interruption or lost income due to a cyber incident
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Timothee Crespe
Cyber Industrial & Materials
Industry Expert
+33 (0)1 4783 0975
timothee.crespe@aon.com

Shannan Fort
Cyber Insurance Leader
Global Broking Centre
+44 (0)20 7086 7135
shannan.fort@aon.com

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

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
- Cost of spoilage

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:

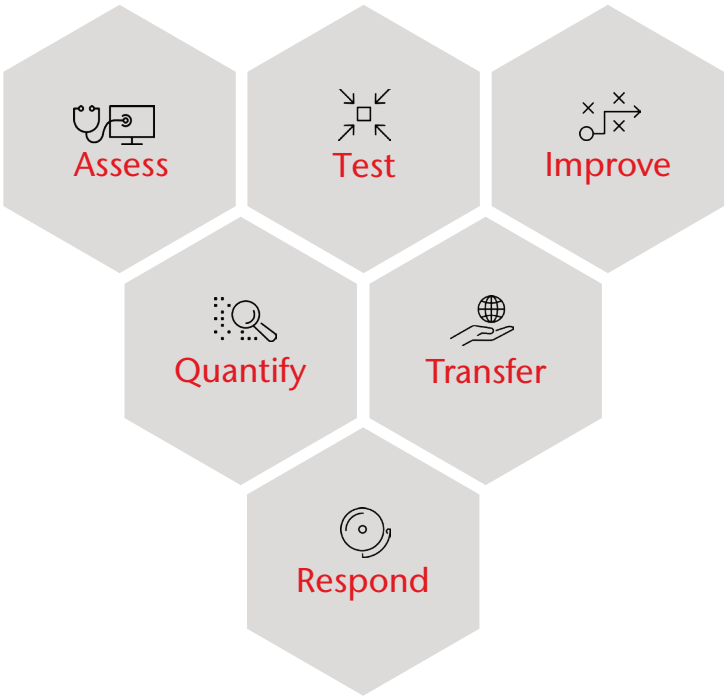
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework 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

An industrial manufacturer domiciled in the UK with global operations made a decision to purchase cyber insurance for the organisation.

Operating across a number of continents with a very complex network topology, the organisation was finding it challenging to centralise the information security control documentation that would be necessary to present the risk to the market.

Aon's experts worked with the client's information security function to prepare an appropriate and proportionate underwriting submission to the market. This articulated the organisational exposures and development workstreams to allow the cyber market to understand the level of cover that would be needed.

We also assisted the Chief Information Security Officer to prepare for any market questions that would be asked.

This process assisted our client in a number of ways and delivered valuable results:

Awareness: Aligned visibility of cyber security risk practices with the insurance and risk management function within the organisation.

Governance: Developed board level awareness of the organisational exposures to cyber risk.

Insurance: Bespoke wording to reflect the uniqueness of the organisation's cyber risk profile, providing very comprehensive insurance coverage and obtaining +£100m of coverage from the marketplace. We also helped the organisation consider future captive utilisation.