Aon
Cyber Solutions

Marine

Cyber risk exposures and solutions

Marine organisations 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 marine organisations:

- Increased dependence on technology for the management of cargo, the bridge, navigation, tracking, propulsion, performance optimisation, communication and entertainment
- Increased connectivity of technologies and connectedness of vessels through satellite communication systems
- Security of IoT devices on board ships is not integrated and typically very weak
- Dependence on vendors, independent contractors or additional service providers

Potential cyber incidents for marine organisations:

- Hackers penetrating navigation & propulsion systems, using on-board systems to:
  - divert and steal cargo
  - take over control of a vessel causing disablement, grounding or collision
  - extort a ransom payment in return for control over the vessel
- Phishing or spear-phishing attacks aimed at crew
- Business interruption or lost income due to a cyber incident
- Bodily injury or property damage resulting from a cyber event
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Maarten van Wieren
Cyber Marine Industry Expert
Industry Expert
+31 (0)68 2019225
maarten.van.wieren@aon.nl

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
- Supply chain business interruption
- Cost of spoilage – replacement of materials that are transferred
- Bricking coverage – replacement costs for portions of fleet (IoT)
- 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:

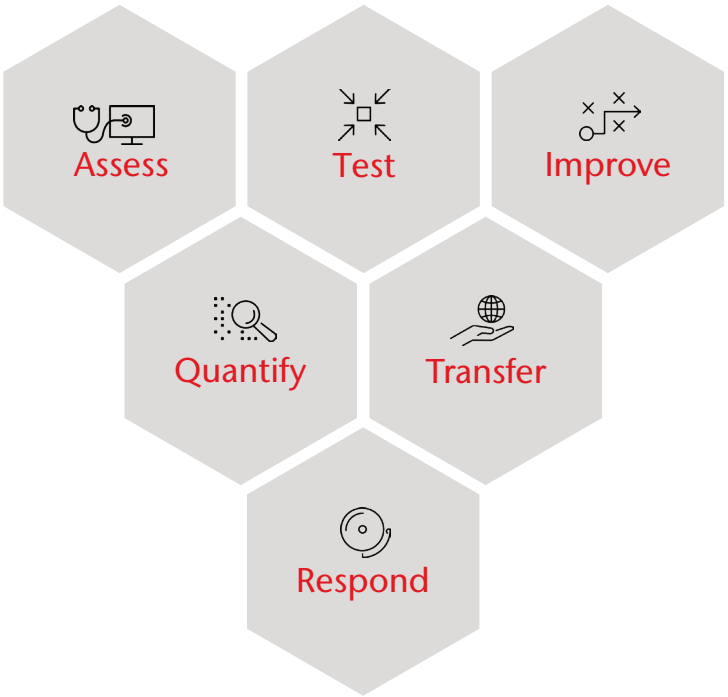
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework supporting organisations 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 from a network security breach, business interruption and extra expense coverage as a result of a systems failure, contingent network business interruption for IT vendors and the supply chain, and cyber terrorism coverage.
- *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

A large UK based conglomerate with some major marine and shipping operations wanted to better understand their overall group cyber exposure.

Operating across a number of continents (Europe, Africa, Asia), the organisation had a relatively unsophisticated IT environment. Despite this it was believed that their cyber risk exposure could potentially be very large as most of their assets and their client assets could potentially be interfered with.

The client asked Aon to assist them in profiling the threat exposures to their organisation and in particular to their shipping entity.

Due to time restrictions we developed a flexible process to assist the group stakeholders with collating and controlling information sources across various territories.

This approach allowed us to develop a coherent cyber risk profile for the client, allowing for oversight and commentary from group senior management.

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

Governance: Board level recognition and understanding of the cyber risk exposures of the business in a financial context. This allowed for greater levels of awareness regarding the risk exposures of the shipping units.

Security: Identification of vulnerable areas in the organisational IT network requiring further investment for security purposes.