Aon
Cyber Solutions

Aviation

Cyber risk exposures and solutions

Aviation organisations are a target for cyber criminals with motives of financial gain via theft of confidential information or money, or of physical harm. 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 aviation organisations:

- IoT as vulnerable vectors
- Points programmes as vulnerable vectors
- Unique complexity of an airline ecosystem
- Supply chain/cargo risk
- Electronic control and data systems of air cargo shipments are considered a soft target for economic criminals due to:
  - High values of cargo
  - Multiple data transfers through different computer systems
  - Insufficient cyber threat information sharing among logistics shareholders

Potential cyber incidents for aviation organisations:

- Hacking of on-board navigation systems
- Bodily injury or property damage resulting from a cyber event
- Business / service interruption or lost income due to a cyber incident
- Breach of private information
- System outage / IT failure due to a cyber attack impacting reservations, check-in and air-traffic control
- Breakdown / loss of functionality of physical assets due to a cyber breach (i.e. baggage and airplanes)
- Business disruption loss as a result of an aerospace manufacturer experiencing a cyber attack
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Shannan Fort
Cyber Aviation 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

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
- Bricking coverage – replacement costs for IoT
- Regulatory fines for delays and cancellations
- Cost of rebooking flights on other airlines & associated passenger expenses

Our approach

Adopting a risk based cyber insurance strategy

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

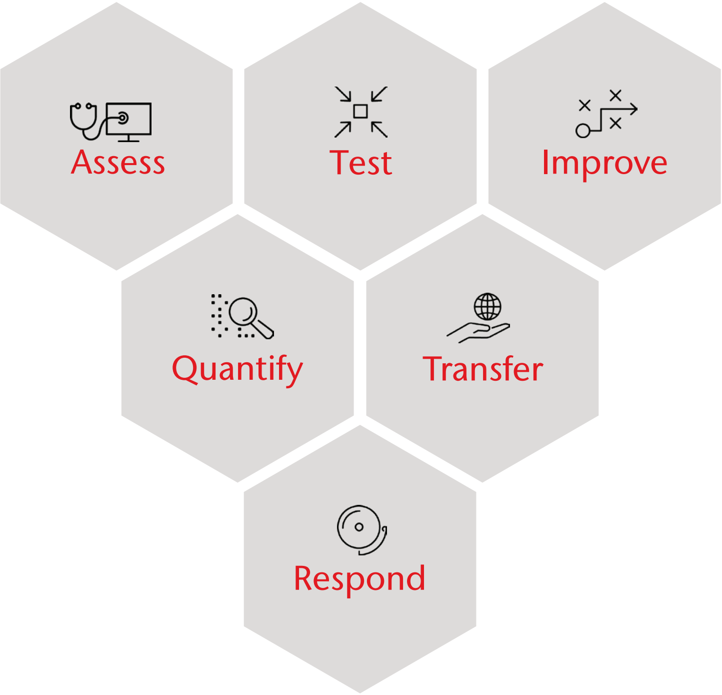
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



Client story

Client Goals

An aerospace organisation in Europe wanted to achieve a better understanding of their cyber threats, determine the balance sheet exposure from those threats and examine methods to mitigate or transfer the risks identified. They engaged Aon to help.

Our Approach

By utilising our experience in information security protection and cyber risk financing, our experts performed a cyber risk assessment and quantification which included the following steps:

1. **Scenario analysis:** As a first step we established and prioritised relevant cyber risk scenarios.
2. **Financial modelling:** We then developed an appropriate model to determine the financial exposures for the aerospace organisation.
3. **Insurability analysis:** Finally, we aligned the insurable risk exposures with the insurance strategy to optimise the total cost of risk.

Result

Results of the assessments were used to report to the Board of Directors on the potentially catastrophic exposures and steps to mitigate these. This supported additional cyber security investments and helped them to ultimately approach cyber as an enterprise risk. The aerospace organisation is now seeking to optimise their cyber risk transfer strategy in association with their insurable cyber risk profile.

Empower Results®