Healthcare

Cyber risk exposures and solutions

Healthcare 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 healthcare organisations:

- Personally identifiable or corporate confidential information in their care
- High dependency on electronic processes and computer networks
- Dependence on vendors, independent contractors or additional service providers
- Increasing digitalisation in the healthcare technology sector
- Internal technology innovation
- Easy access to buildings
- Privacy regulation

Potential cyber incidents for healthcare organisations:

- Hackers targeting sophisticated control systems
- Life threatening outages
- Spoiling of medicine or blood preservation due to an outage of cooling systems
- Loss of sensitive data
- Social engineering
- Dependent or contingent business interruption due to a cyber event suffered by a third party vendor or supplier
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Johannes Behrends
Cyber Healthcare Industry Expert
+49 (0)208 7006 2250
johannes.behrends@aon.de

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 to re-perform research, including clinical trials
- Contingent bodily injury and property damage
- Medical identity theft monitoring and insurance for affected individuals
- Bricking cover extended to medical devices

AON
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:

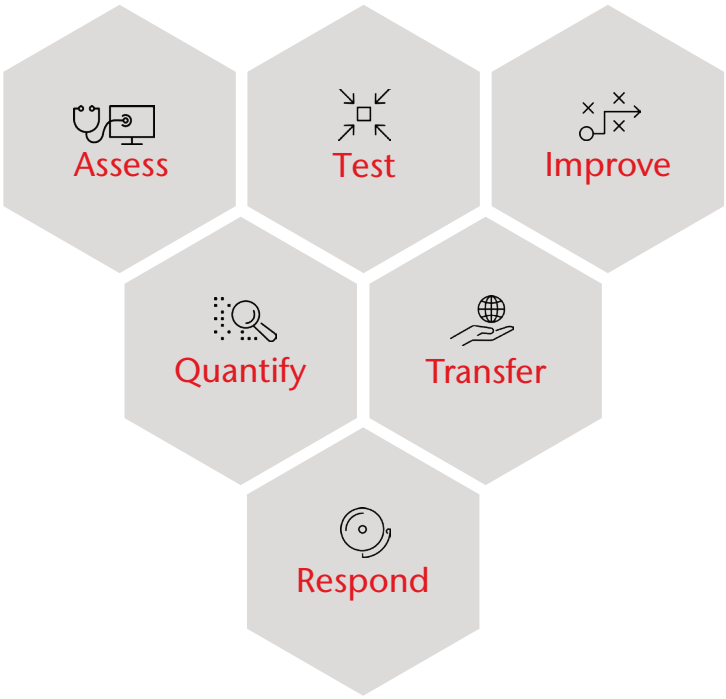
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework 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 not-for-profit healthcare system with multiple facilities in inner city and suburban locations was experiencing significant physical and information security-related challenges. Most notably, these included the physicians' need for remote, mobile access to highly confidential medical records and maintenance of disparate sources of confidential information with varying governance processes. Compounding this was a lack of communication across security functions and limited threat awareness among the employee and physician population. The client hired Aon to perform a comprehensive security risk assessment spanning both physical and electronic security departments.

Our technical specialists at Stroz Friedberg identified systemic risk issues pertaining to the organisational culture, security governance, business practices, and the physical security of information assets. We then provided a comprehensive report describing security findings and prioritised recommendations for remediation. Not only did Stroz Friedberg's recommendations include technical and procedural security defence fortifications, but they also focused on improving the channels of communication between physical and information security entities, and provided a strategy to enhance employee and physician awareness of current security threats and best practices.

Our knowledge of the healthcare industry positioned us to confidently communicate critical industry specific issues throughout the organisation, including to the board. Our ability to align the client's risk tolerance with industry regulation, improve governance standards, and develop a communications process ultimately increased the internal reputations of the physical and IT security departments and limited the risk for an incident.