

Retail

Cyber risk exposures and solutions

Retail 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 retail organisations:

- ▶ Gathering, maintaining, disseminating or storage of private information
- ▶ Retailers are responsible for the vast amounts of payment card information that flows through their systems and are subject to the rules and regulations of the Payment Card Industry and other regulatory bodies
- ▶ High dependency on electronic processes or computer networks
- ▶ Dependence on vendors, independent contractors or additional service providers
- ▶ Frequent technological advances in the POS space create efficiencies in the payment process, however, open new vulnerabilities
- ▶ New mandates and standards (EMV chip-compliance) are frequently being introduced to the retail sector and often require immediate attention
- ▶ Subject to regulatory statutes
- ▶ Privacy regulation

Potential cyber incidents for retail organisations:

- ▶ Hackers targeting Point-of-Sale systems (POS) or third party vendors to gain access to retailers' network
- ▶ Unauthorised access to online sales operations
- ▶ Exposed credit card information
- ▶ Intentional acts committed by rogue employees
- ▶ Ransomware attacks

We're here to empower results

Rachel Phillips
Cyber Retail Industry Expert
rachel.phillips2@aon.co.uk
+44 (0)20 7086 0411

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

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 | • No failure to patch exclusion |
| • Broad definition of computer system | • Full limits for Payment Card Industry (PCI) |
| • Coverage for cyber terrorism | • Identity theft coverage as part of the credit monitoring |
| • Deletion of the unencrypted device exclusion | • Full limits for goodwill coupon |
| | • Environmental liability |

Our approach

Adopting a risk based cyber insurance strategy

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

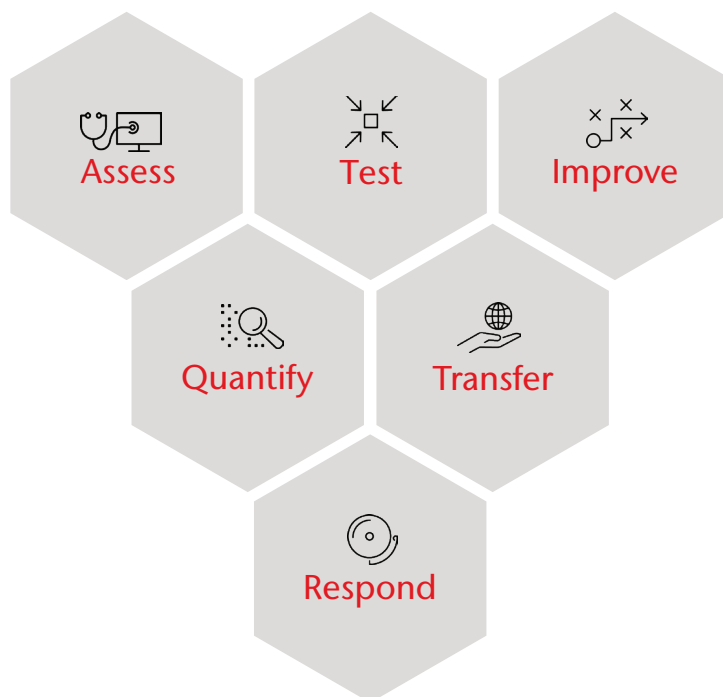
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



Client story



In light of significant cyber incidents that had impacted the retail industry, a multinational supermarket chain with operations on three continents wanted to purchase cyber insurance as a matter of urgency.



Cyber risk assessment and risk transfer

Given the complex IT infrastructure of the client with retail and supply chain operations across the US, EMEA and APAC, our experts employed Aon's Cyber 360 platform to establish and prioritise relevant risk scenarios for the organisation.

As a second step, we developed a model to determine the loss exposure, to then align the insurable risk exposures with an optimised insurance strategy for the organisation.



The result of this structured approach enabled us to place a limit in the hundreds of millions in one month, while optimising coverage tailored to the specific exposures of this retail chain.

Aon UK Limited is authorised and regulated by
the Financial Conduct Authority. FP.AGRC.194.SM

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.