

Professional Services

Cyber risk exposures and solutions

Law firms, accountants, and other specialised consultancy firms 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 professional services organisations:

- ▶ Personally identifiable or corporate confidential information in their care
- ▶ Damage to reputation
- ▶ Interruption to business / prevention from operation
- ▶ Internal technology innovation
- ▶ Privacy regulations
- ▶ High dependency on electronic processes and computer networks
- ▶ Regulatory oversight resulting in fines and penalties
- ▶ Dependence on vendors, independent contractors or additional service providers

Potential cyber incidents for professional services organisations:

- ▶ Theft and potential release of personally identifiable or corporate confidential information in their care
- ▶ Malware preventing access to systems and causing interruption to business
- ▶ Social engineering
- ▶ Network disruption
- ▶ Insider access
- ▶ Cyber incident affecting a crucial outsourced service provider
- ▶ Intentional acts committed by rogue employees
- ▶ Ransomware attacks

We're here to empower results

Jonathan Breaden
Cyber Professional Services
Industry Expert
+44 (0)20 7086 1011
jonathan.breaden@aon.co.uk

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
- Broad definition of computer system
- Coverage for cyber terrorism
- Deletion of the unencrypted device exclusion
- No failure to patch exclusion
- Combine with Errors & Omissions coverage
- Coverage for in-house forensics and other in-house services

Our approach

Adopting a risk based cyber insurance strategy

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

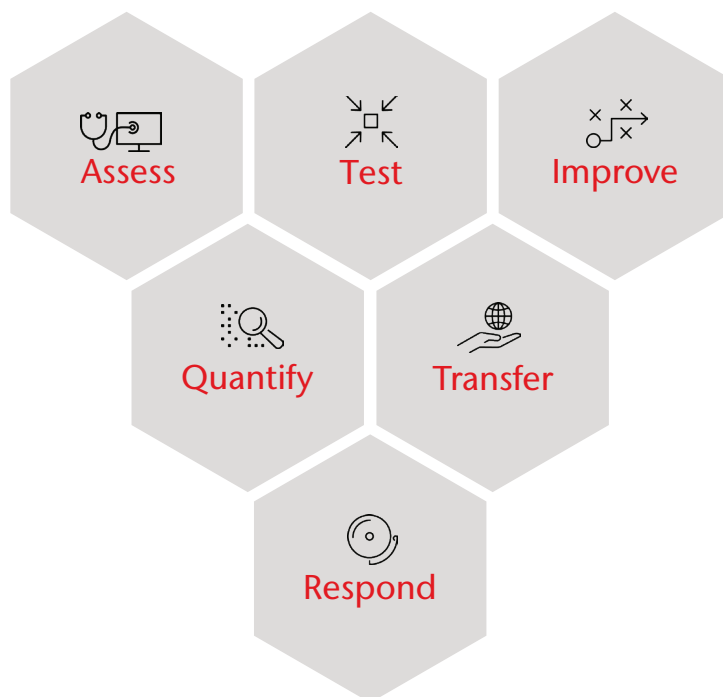
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



A UK law firm wanted to purchase a cyber insurance policy, but lacked understanding of the following:

- Cyber coverage they already had under their existing insurance policies
- What cyber coverage was available
- How a cyber policy could assist them in the event of a cyber incident

By utilising Aon's experience in cyber related risk and insurance, our experts performed a cyber risk assessment and quantification which included the following steps:



1. **Gap analysis:** As a first step we reviewed the firm's existing insurance policies, and provided a guide to what cyber risks were covered by their existing insurance and what areas were not.
2. **Understanding cyber risks:** We provided an overview of cyber risks, the cover available under a cyber insurance policy, and a detailed claims scenario that highlighted how a cyber insurance policy would respond to the various losses and costs of a cyber event.
3. **Placing the insurance:** We obtained underwriting information from the client, secured cyber insurance terms from a number of insurers and provided a comprehensive analysis, which included a detailed wording comparison.
4. **Understanding expectations:** We facilitated a meeting between the insured and the chosen primary insurer prior to inception, to understand how a cyber policy would respond in the event of a claim, including crisis management.



Following the cyber risk assessment and quantification, the law firm was able to make informed decisions on:

Insurance: We secured the client broad levels of coverage at a competitive premium, with bespoke policy wording reflecting what cyber risk represented to the law firm.

Cyber risk management: As a result of buying insurance, the law firm benefited from our cyber risk management services and expertise, and further developed their relationship with the insurer.

Aon UK Limited is authorised and regulated by
the Financial Conduct Authority. FP.AGRC.181.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.