Aon
Cyber Solutions

Public Sector

Cyber risk exposures and solutions

Public sector organisations such as the civil service, military, police, infrastructure and governmental agencies 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 public sector organisations:

- Gathering, maintaining, disseminating or storage of private information
- High dependency on electronic processes or computer networks
- Relying on or operating critical infrastructure
- Mandated record retention periods
- Outdated IT infrastructure and budgetary limitations
- Engaging vendors, independent contractors or additional service providers
- Privacy regulation

Potential cyber incidents for public sector organisations:

- Hacktivist activity
- Bodily injury or property damage resulting from a cyber event
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

Alexander van Nierop
Cyber Public Sector Industry Expert
+31 (0)1 0448 7131
alexander.van.nierop@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

AON
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
- Property damage
- Business interruption
- Business interruption liability
- Costs incurred to purchase power/energy from other sources (spot markets)
- Environmental liability

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:

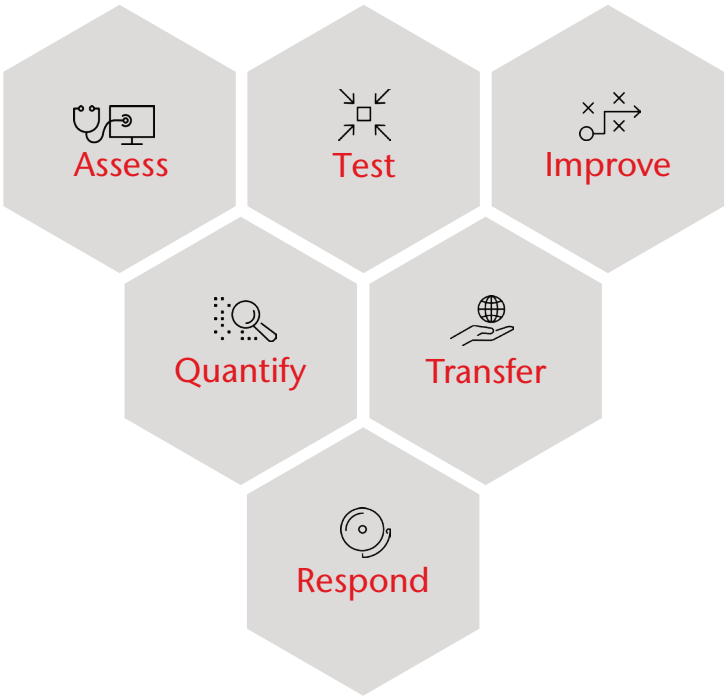
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



Empower Results®

Client story

Recently, a municipality suffered from an immense cyber attack. At least 20 gigabytes of personal data were sent to an unknown site by means of malware. The client had been considering buying cyber insurance in the past, but were still reviewing the added value of this in combination with an assessment of their risk exposures.

Following the incident, the municipality asked Aon for help. We identified their risks to help the organisation understand what risks to retain, which measures to take and which risks to transfer to the insurance market.
By utilising our experience in information security protection and cyber quantification, our experts performed a cyber risk assessment and quantification, and carried out various crisis management simulation trainings, which included the following steps:

1. **Scenario analysis and quantification:** Based on a thorough evaluation of the identified risks and loss scenarios we provided better insight into the most important and highest impacting scenarios for the municipality.
2. **Crisis training:** On the basis of these scenarios various crisis management simulation trainings were organised for key employees to help the municipality be better prepared for future incidents and attacks. Furthermore, they are now more aware of what risks to prioritise.
3. **Insurability analysis:** We aligned their insurable risk exposures with their insurance strategy to optimise the organisation's total cost of risk.

Following the scenario analysis and quantification and the insurability analysis, the municipality could make informed decisions on:

Insurance: We secured the client adequate levels of coverage and a policy wording that reflected what cyber risk represented to the municipality and in line with their specific risk tolerance level.

Crisis management simulation trainings: The trainings carried out helped the client to identify and improve weak spots in their organisation. As a result, they also implemented an employee awareness programme.