

# Energy

## Cyber risk exposures and solutions

Energy 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 energy organisations:

- ▶ Gathering, maintaining, disseminating or storage of private information
- ▶ High dependency on electronic processes or computer networks
- ▶ Contingent bodily injury and property damage resulting from cyber incidents
- ▶ Utilisation of "the cloud" exposes contractors to liability ranging from data security, network outages and regulatory compliance issues
- ▶ Relying on or operating critical infrastructure
- ▶ Evolving regulatory environment potential fines and the need to comply with industry security standards
- ▶ Subject to regulatory statutes
- ▶ Dependence on vendors, independent contractors or additional service providers
- ▶ Vendor held information:
  - Building Information Modelling (BIM) programmes
  - Laptops and portable devices (i.e. iPhones, iPads) to access systems from third party locations such as job sites or hotels

### Potential cyber incidents for energy organisations:

- ▶ Hackers targeting sophisticated industrial control and data acquisition systems
- ▶ Network interruption resulting in lost business income
- ▶ Dependent or contingent business interruption due to a cyber event suffered by a third party vendor or supplier
- ▶ 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 Curtis**  
Cyber Energy Industry Expert  
+44 (0) 20 7086 7164  
alexander.curtis@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 | • Property damage  |
| • Broad definition of computer system   | • Business interruption  |
| • Coverage for cyber terrorism  | • Business interruption liability  |
| • Deletion of the unencrypted device exclusion                                    | • Costs incurred to purchase power/energy from other sources (spot market) |
| • No failure to patch exclusion   | • 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:

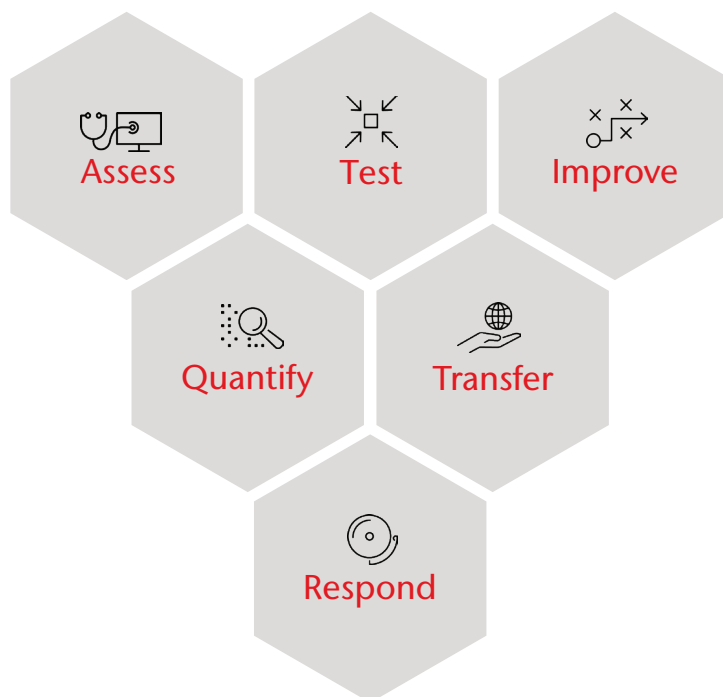
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



With the sector witnessing significant cyber attacks in the last few years, a developer and owner of renewable power assets wanted to regain control of its exposure to cyber risk.

The client requested Aon to provide a consistent approach to identify, quantify, and define the insurability of its cyber exposures both at a group IT level and across its portfolio of power assets.

Exposure to offshore wind assets in particular represented a material threat to the corporate balance sheet. With the proliferation of IoT technology and increased connectivity of SCADA and Industrial Control Systems (ICS), the company realised its key technological assets were susceptible to cyber risk.

The client looked to use us to provide direction in quantifying their top exposures, with a view to using the analysis to develop a bespoke cyber insurance policy spanning all offshore power assets.



To achieve the stated objectives, we employed our proven framework through a three-staged approach.

Our team held a one-day workshop with the client to establish key IT, OT systems and data assets and prioritise cyber risk scenarios with input from SCADA / ICS, group IT and operations teams.

We worked with a specialist in-house risk control engineering resource to verify scenarios and develop an appropriate model to calculate their financial impact.

An insurability analysis was then conducted, leveraging knowledge from power and cyber insurance experts to align insurable risk exposures with an optimised insurance strategy.



This process assisted our client in a number of ways and delivered valuable results:

**Awareness:** Through this engagement, the client determined its balance sheet exposure from cyber risks and could clearly differentiate between transferable risks and those retained by the business.

**Insurance:** Following the review, the client engaged directly with Aon's broking team to help articulate its cyber risk profile to the insurance market. The assessment was used directly to inform bespoke wording, reflecting the uniqueness of the organisation's cyber risk profile.

**Cybersecurity:** For non-insurable risks, the client implemented stronger controls around key exposures. This included data classification by sensitivity, value and criticality alongside proactive log monitoring.

Aon UK Limited is authorised and regulated by  
the Financial Conduct Authority. FP.AGRC.184.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.