



# Life Sciences & Pharma

## Cyber risk exposures and solutions

Life sciences & pharma 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 life sciences and pharma organisations:

- ▶ Personally identifiable or corporate confidential information in their care
- ▶ Increasing digitalisation in the life sciences & pharma technology sector
- ▶ High dependency on electronic processes and computer networks
- ▶ Internal technology innovation
- ▶ Dependence on vendors, independent contractors or additional service providers
- ▶ Privacy regulation

### Potential cyber incidents for life sciences and pharma organisations:

- ▶ Hackers targeting sophisticated control systems
- ▶ Dependent or contingent business interruption due to a cyber event suffered by a third party vendor or supplier
- ▶ Loss of sensitive data
- ▶ Intentional acts committed by rogue employees
- ▶ Social engineering
- ▶ Ransomware attacks

### We're here to empower results

**Anne-Christine Fischer**  
Cyber Life Sciences Industry Expert  
+49 (0)208 7006 2810  
[anne-christine.fischer@aon.de](mailto:anne-christine.fischer@aon.de)

**David Molony**  
Cyber Risk Leader  
Cyber Solutions EMEA  
+44 (0)777 5227008  
[david.molony@aon.co.uk](mailto:david.molony@aon.co.uk)

**Spencer Lynch**  
Cyber Security Leader  
Cyber Solutions EMEA  
+44 (0)20 7061 2304  
[spencer.lynch@aon.co.uk](mailto:spencer.lynch@aon.co.uk)

**Vanessa Leemans**  
Chief Broking Officer  
Cyber Solutions EMEA  
+44 (0)20 7086 4465  
[vanessa.leemans@aon.co.uk](mailto:vanessa.leemans@aon.co.uk)

**Richard Hanlon**  
Chief Commercial Officer  
Cyber Solutions EMEA  
+353 (0)1 266 6443  
[richard.hanlon@aon.ie](mailto:richard.hanlon@aon.ie)

[aon.com/cyber-solutions](https://aon.com/cyber-solutions)

# 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 with insurers (subject to market agreement per individual risk):

- |   |  |
|---|--|
| • Full limits for incident response and costs associated with breach notification | • Cost to re-perform research, including clinical trials                   |
| • Broad definition of computer system   | • Contingent bodily injury and property damage                             |
| • Coverage for cyber terrorism  | • Medical identity theft monitoring and insurance for affected individuals |
| • Deletion of the unencrypted device exclusion                                    | • Bricking cover extended to medical devices                               |
| • No failure to patch exclusion   |  |

# Our approach

## Adopting a risk based cyber insurance strategy

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

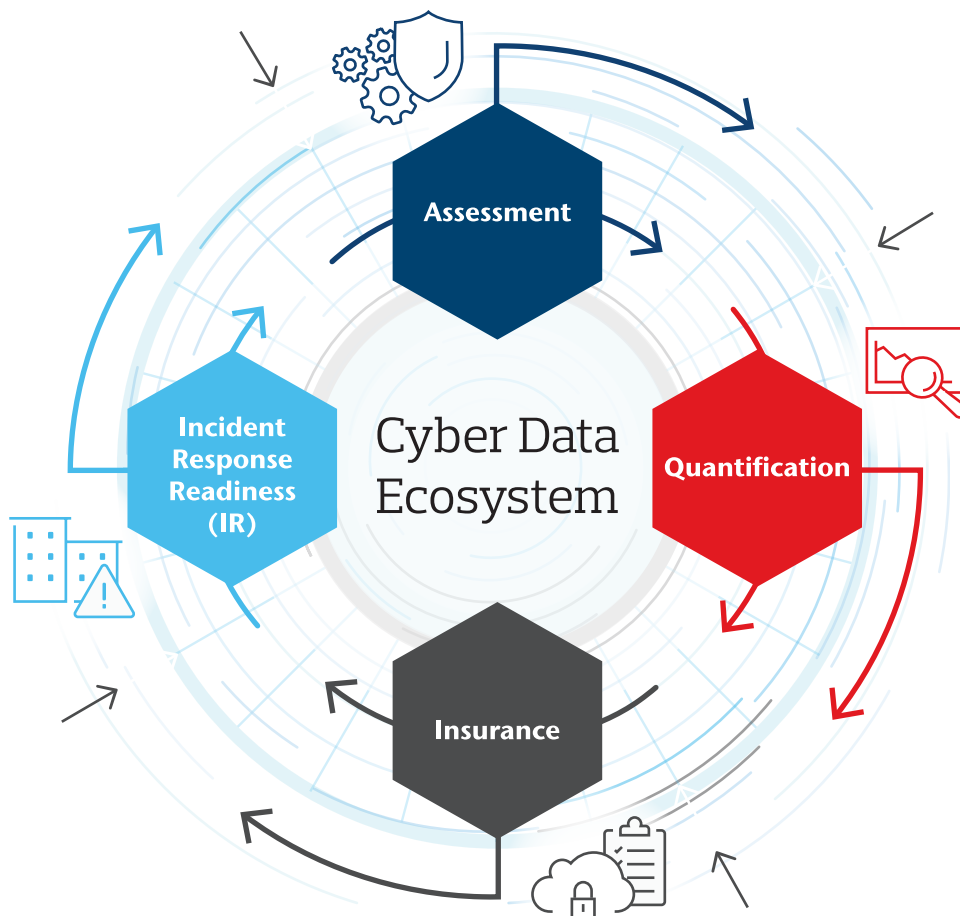
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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

## The Cyber Loop: a continuous response to an evolving threat

Aon's Cyber Solutions offers a full range of services to help you understand and manage cyber as an enterprise risk.



# Client story



A large pharmaceutical organisation was becoming increasingly concerned about their exposure to cyber risk. Operating across a number of continents with a very complex network topology, the organisation was finding it difficult to centralise the information security control documentation that would be necessary to present the risk to the market.

The client was also unable to quantify their cyber exposures and did not have an appropriate indicator as to the level of cover that may be required.



Based on the network exposure identification, Aon developed a model to quantify the loss exposure and aligned the insurable risk exposures with an optimised insurance strategy for the organisation.

We involved stakeholders from across the organisation to create clear line of sight on the organisational cyber exposures.



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

**Governance:** Board level recognition and understanding of the cyber risk exposures of the organisation in a financial context. The board sanctioned a capital expenditure for the organisation to procure cyber insurance for the first time.

**Insurance:** Bespoke wording reflecting the uniqueness of the organisation's cyber risk profile providing very comprehensive insurance coverage and obtaining +£200m of coverage from the marketplace.

**Security:** Identification of vulnerable areas in the organisational IT network requiring further investment for security purposes.

## About Aon's Cyber Solutions:

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

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.

Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services.  
FP.AGRC.395.AP

The following products or services are not regulated by the Financial Conduct Authority:

- Cyber risk services provided by Aon UK Limited and its affiliates.
- Cyber security services provided by Stroz Friedberg Limited and its affiliates.

Aon Belgium B.V. is authorised and regulated by the Belgian Financial Services and Markets Authority ("FSMA").

© Aon plc 2021. All rights reserved.