Aon
Cyber Solutions

Higher Education

Cyber risk exposures and solutions

Higher education 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 higher education organisations:

- Gathering, maintaining, disseminating and storing private information
- Collecting financial and sensitive information through campus bookstores and student health clinics
- High dependency on electronic processes or computer networks
- Engaging vendors, independent contractors or additional service providers
- Holding sensitive intellectual property that potentially has significant commercial value
- System failure at point of admissions process
- Subject to regulatory statutes

Potential cyber incidents for higher education organisations:

- Hacktivist activity
- Misappropriation of student course work or exam papers
- Intentional acts committed by rogue employees or students
- Ransomware attacks

We're here to empower results

Jeffrey Jolliffe
Cyber Higher Education Industry Expert
+44 (0)20 7086 0423
jeffrey.jolliffe@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

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
- Amend exclusions so Reg cover applies even if it is your Regulatory Body
- Consider group programmes as systems may overlap
- Risk retention groups/pools for group purchasing with other state / government owned schools
- Turn-key approach – BBR
- Extend cover for university if student/faculty causes third party breach
- Cost to restore data belonging to students & faculty and re-perform research

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:

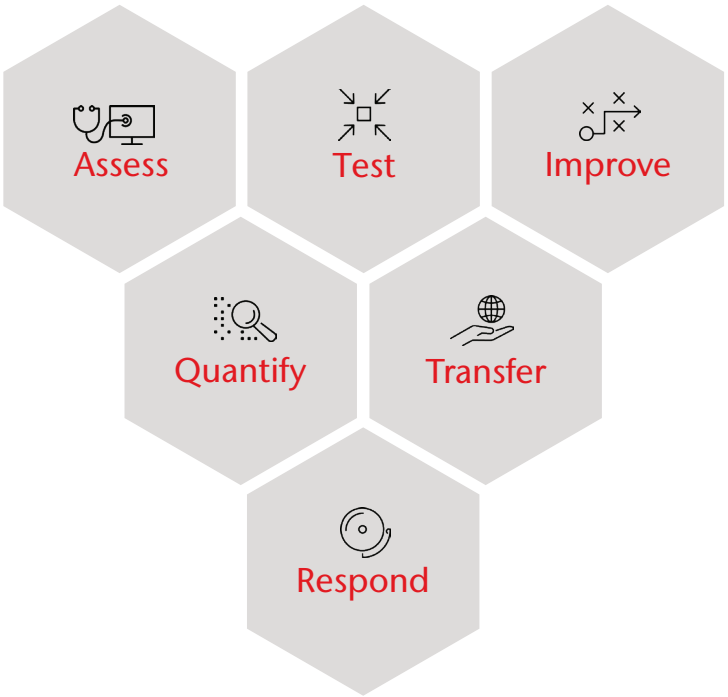
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework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



Empower Results®

Client story

A university in Europe asked Aon to review their existing cyber insurance programme. They wanted to obtain assurance on the appropriateness of their limits and coverage to adequately respond to a data breach. While they wanted to optimise their cyber insurance programme, their insurance budget remained unchanged.

Our brokers reviewed the university's current policies and structure to provide commentary. While it was clear their broker at the time (another top tier competitor) had scrutinised and improved coverage over the years, Aon was still able to point out deficiencies that could greatly improve the programme.

Our experts performed a cyber risk assessment and quantification which included the following steps:

1. **Scenario analysis:** As a first step, we established and prioritised relevant cyber risk scenarios.
2. **Financial modelling:** We then developed an appropriate model to determine the financial exposures for the university.
3. **Risk transfer review:** Through modelling of cyber loss scenarios and stress testing current limits, it became clear that the probable maximum loss of a cyber incident was higher than their existing cyber insurance limit. The breach costs sublimit structure was also not suitable for an organisation of their size.

Following the cyber risk assessment and quantification, the university decided to increase the limit of their cyber insurance programme and to include full coverage for breach costs. We then performed a marketing effort, taking great care to ensure the client had face-to-face meetings with each carrier. We restructured the excess layers, which led to a price decrease. With those extra funds, the client chose to add a further €10M in limit to their insurance programme.