Higher Education
Cyber Risk Exposures and Solutions

Cyber risk refers to the loss potential an organization faces by virtue of holding confidential information as well as relying on information technology, connectivity and automated processes. While improved efficiency and security is derived from technology implementation, organizations face additional risk from the cyber exposures inherent in their technology systems. In an increasingly punitive legal and regulatory environment, and in the face of more frequent external requirements for cyber liability insurance, forward-thinking organizations are taking proactive steps to explore and transfer cyber risk.

Higher education institutions face a number of inherent security & privacy exposures:

- Gathering, maintaining, disseminating and storing private information on students, alumni, faculty, season ticket holders, and applicants
- Collecting financial and healthcare information through campus bookstores and student health clinics
- Relying on electronic processes or computer networks to educate students
- Utilizing vendors, independent contractors or additional service providers who have access to confidential information and critical systems

Higher education cyber concerns:

- The general user base is highly innovative, technically adept & highly unpredictable
- Educational institutions are open and collaborative, which is designed to allow the free flow of ideas and information, but introduces significant vulnerabilities related to information security
- Networks are intentionally porous to allow access by default and deny access by exception
- Legacy systems and applications frequently no longer have IT support from technology provider
- Sensitive third party data that goes beyond personal and financial information (particular focus on institutions with strong engineering and computer science departments)
- Educational institutions are subject to regulatory statutes including HIPAA and FERPA

Scope of cyber coverage available in the insurance marketplace:

Third Party Coverage Elements

- Security and privacy: defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, denial of service attack or transmission of a computer virus
- Regulatory defense and fines: defense 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: defense 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: defense costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

We're here to empower results

If you have any questions about your specific coverage or are interested in obtaining coverage please contact your Aon broker or visit **aon.com.**

The Aon acquisition of **Stroz Friedberg** enhances the ability of Aon to support clients with leading digital forensics and incident response capabilities.

Empower Results®

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 center, identity theft resources
- 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
- 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: 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

How do organizations transfer cyber risk?

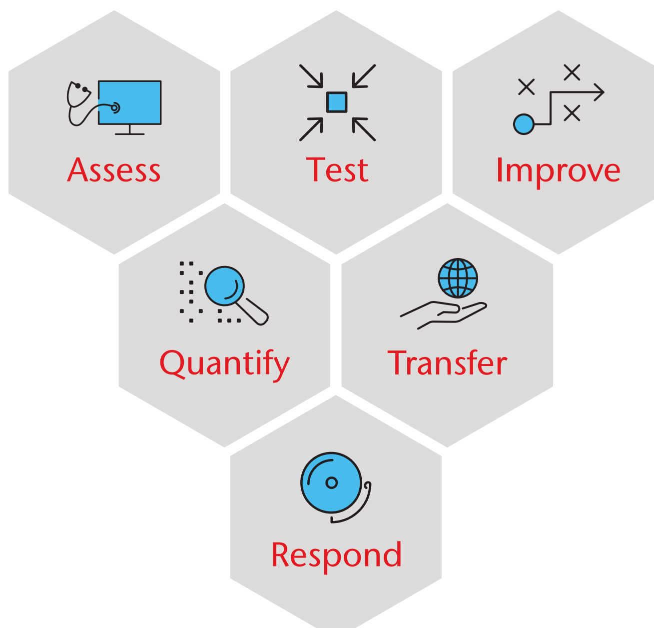
- The cyber insurance marketplace provides service solutions, including loss control resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response
- The scope of breach response coverage offerings varies based on insurer and policy structure
- 60+ insurers provide cyber coverage with large capacity available

Aon Cyber Innovation

The Aon Cyber Enterprise Solution is a first-of-a-kind policy that 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. This product provides catastrophic limit in excess of $400M USD.

The Aon Approach

Aligned with client's risk management approach to cyber security, Aon's approach supports a risk-based methodology to risk financing and insurance arrangements, ultimately helping clients optimize the total cost of risk associated with cyber exposures. To achieve this, Aon recommends the following process:



Empower Results®