MIDWESTERN HIGHER EDUCATION COMPACT

Cyber Insurance

A Midwestern Higher Education Compact Program

HIGHER EDUCATION THREAT HORIZON AND INDUSTRY OUTLOOK

Higher education institutions continue to face significant cyber threats due to the valuable information stored on their networks and the ability for threat actors to use network infrastructure to launch operations against other targets. College and university networks can be difficult for administrators to effectively secure because of their size and the number of users as well as the need for internal and external users to access and share information.

THE FOLLOWING FACTORS MAY ALSO INCREASE THREAT ACTIVITY

RESEARCH PROGRAMS

Research with a potentially high economic payoff or that supports sensitive government research contracts may lead to increased targeting from cybercriminals. In particular, advanced persistent threat (APT) groups often search for intelligence to benefit their sponsoring government or associated state-owned companies.

PROMINENT FACULTY

Association with high profile or influential academics or dissidents may result in a greater threat activity from APT groups. These groups often seek to gather information that would allow their sponsoring government to monitor that individual's activity and gain insight into policy discussions.

SYMBOLIC TARGETS

Targets that are perceived to be highly visible or symbolic may lead to threat activity from hacktivists or APT groups seeking to disrupt website or network operations for political purposes.

CONTROVERSY

Involvement in controversy may lead to threat activity from hacktivists seeking to protest and embarrass the victim organization through disrupting website access, defacing webpages, or stealing and exposing the organization's sensitive information.

STATE SPONSORED ATTACKS

State sponsored attacks continue to be a concern, with state sponsored threat actors accounting for over 50% of higher education breaches.

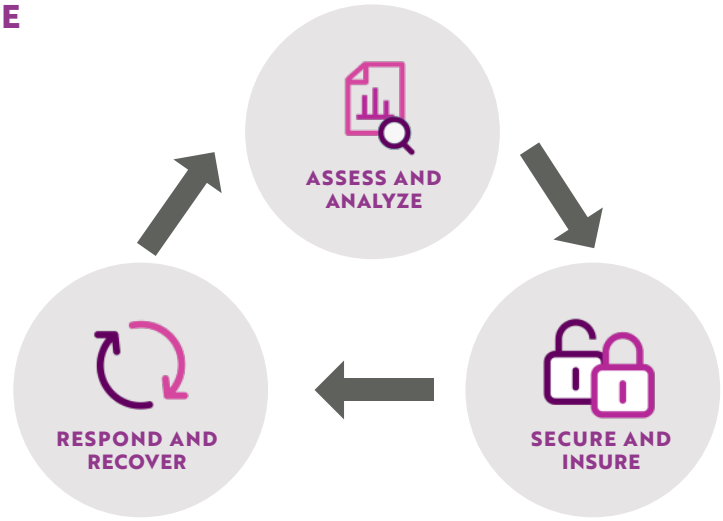
CYBER RISKS

Each institution has unique cyber risks because of their business operations, assets, and threat environment. The institution's use of technology within its operations and any handling/collection/storage of confidential information contribute to the ongoing battle of keeping the institution's assets safe from threat actors.

The MHEC Cyber Insurance approach analyzes the institution's threat environment, assesses the significance of the vulnerabilities in security controls, and determines how much financial exposure the institution faces. MHEC's approach can also provide benchmarking on how much cyber coverage institutions of similar risk are buying.

EXAMPLES OF CYBER RISK INCLUDE

- Cyber-extortion
- Cyber-terrorism
- Loss of revenue due to a computer attack
- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches of confidential information



RISK TRANSFER

Insurance Coverages

What options are available to transfer institutional economic risk? What is the typical reach and extent of cyber coverage, as it relates to other lines?

COVERAGE	DESCRIPTION
Network Security Liability	Harm suffered by others from a failure of network security.
Privacy Liability	Harm suffered by others due to the disclosure of confidential information.
Notification Costs	The cost of complying with the various breach notification regulations with a remedy.
Regulatory Defense	Legal defense for regulatory actions (EU's General Data Protection Regulation, FERPA, HIPAA).
Property Loss – Data Asset	The costs to recreate data stolen, destroyed, or corrupted by a computer attack.
Loss of Revenue – Network Interruption	Business income that is interrupted by (1) a system outage or (2) failure of a BPO-cloud provider, including extra expense.
Cyber-Extortion	The cost of investigation and the extortion demand.
Professional Liability	Harm suffered by others due to the negligence in rendering a service and/or a product's failure to function as intended.
Media Liability	Harm suffered by others due to an infringement of an intellectual property right.

MHEC CYBER INSURANCE APPROACH

Institutions in the MHEC member states have been asking for a cyber insurance solution which is tailored to deliver the right mix of risk transfer and advisory solutions for institutions to assess, manage, and respond to their risk. Along with MHEC's Master Property Program administrator, Marsh, MHEC is able to offer institutions the flexibility of insurance carrier choice, the broadest coverage available, and access to limits that meet institutional coverage needs. MHEC will work to build a critical mass of participating institutions to provide a potential option of risk sharing in an excess layer of coverage. This shared excess layer would afford additional coverage at a reduced cost versus an institution securing coverage on a stand-alone basis.

As a market leader higher education marketplace, Marsh's cyber insurance specialists understand the unique risk factors of higher education and are well positioned to:

Assess and Analyze

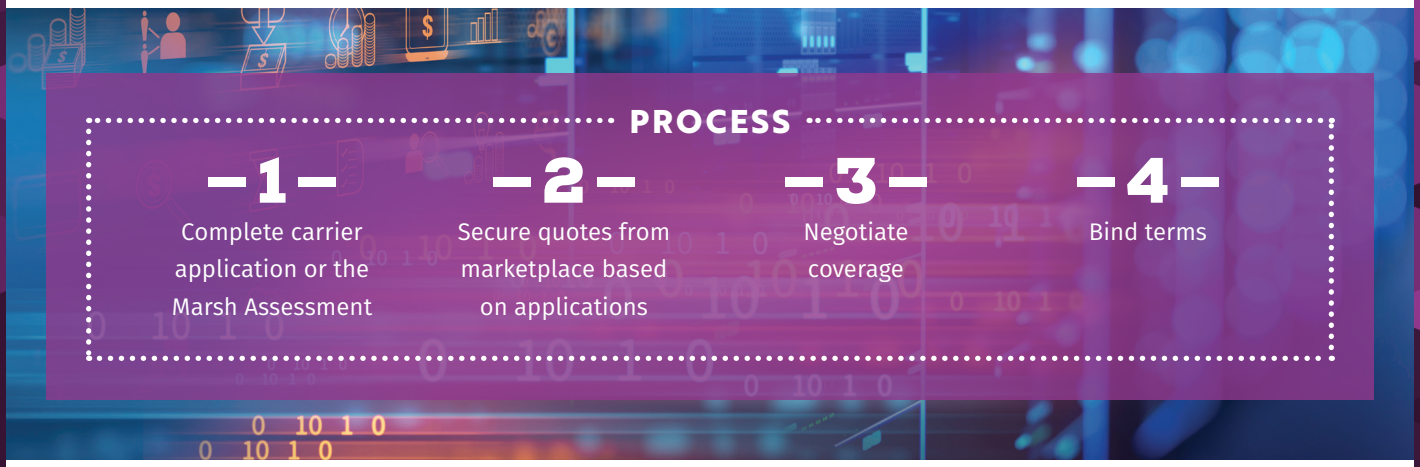
Understand attack scenarios and risk profile when addressing cyber risks.

Secure and Insure

Managing cyber risks means preparing institutions for the inevitable event. Marsh's cyber team will work with institutions to optimize the security controls that protect and detect threats, and transfer exposures off the institution's balance sheet.

Respond and Recover

Quick, effective response to a cyber event is crucial for business. Marsh's cyber team will guide and support institutions through the event, and enhance protection moving forward.



CONTACT

FRANK D. CELLA, *Managing Director*
(312)627-6082 *office* | (847)644-5143 *cell*
Frank.D.Cella@marsh.com

MARSH *Education Practice Leader*
540 W Madison, Ste 1200 Chicago, IL 60661
www.marsh.com

MIDWESTERN HIGHER EDUCATION COMPACT

MIDWESTERN HIGHER EDUCATION COMPACT
105 Fifth Avenue South, Suite 450 Minneapolis, MN 55401
PHONE: (612)677-2777 **FAX:** (612)767-3353 **E-MAIL:** mhec@mhec.org

May 2018