Cyber Liability Insurance FAQ

A Higher Education Information Security Council (HEISC) Resource

September 2015

HIGHER EDUCATION INFORMATION SECURITY COUNCIL

EDUCAUSE

Cyber Liability Insurance

The interest in cyber liability insurance has increased in response to high-profile data breaches making headline news. The market is evolving and nonstandard. The terms and conditions are complex and require thorough analysis prior to purchasing. This resource is designed to assist organizations that are considering purchasing cyber liability insurance.

Key Findings from a March 2015 URMIA Member Survey on Cyber Liability Insurance

From the 109 survey responses, the key findings of the survey are:

- About 68% of respondents purchase cyber liability insurance, with about 70% having done so within the last three years. Those who do not purchase a cyber policy are reevaluating their decision.
- Respondents from private institutions purchase cyber liability insurance more often than those from public institutions, while smaller institutions purchase cyber liability insurance more often than larger ones. Private institutions purchase higher limits than public institutions, as do larger institutions than smaller.
- Most institutions that purchase a cyber policy have limits of $5 million or less and deductibles of $50,000 or less.
- In their purchasing decisions, institutions value insurer coverage of the cost of data breach notification and credit monitoring and assistance with complying with notification laws for multiple jurisdictions.
- Nearly a third of the respondents have filed a claim under their cyber liability insurance and have been satisfied with the insurer's response.

Disclaimer

Purchasing cyber liability insurance is not a substitution for building and improving your information security program. Most policies will require an attestation to the maturity of your information technology and information security programs prior to issuing the policy. Some companies may require an independent audit of your IT and IT security program before issuing a policy. In some cases, the questionnaire or audit process may help you determine priorities for investing in your security program prior to purchasing insurance.

Common Reasons Organizations Purchase Cyber Liability Insurance

1. To reduce the financial burden of notification costs, in the event of a data breach.
2. As a one-stop shop for breach notification, crisis management, and public relations.
3. To access specialized investigative and forensic services.

Who Should Be Involved in the Discussion?

- Chief information security officer (CISO), or equivalent
- Chief risk officer (CRO), or equivalent
- Chief information officer (CIO), or equivalent
- Chief financial officer (CFO), or equivalent
- Chief privacy officer (CPO), or equivalent
- Registrar or other data steward representatives
- Compliance officer, or equivalent (may include those responsible for PCI DSS or HIPAA)
- Procurement officer
- Advancement or alumni representative
- University communications representative
- Legal/general counsel

Considerations When Researching Cyber Liability Insurance

- Investigate what risks are covered by your existing insurance packages. There may be overlaps with a cyber insurance policy.
- Calculate your institution's potential exposure by looking at how much personally identifiable information (PII) or personal health information (PHI) your institution has.
- Carefully examine the policy's requirements and exclusions.
- Determine whether the policy requires the use of a particular company for forensic and investigation services. To avoid invalidating the policy, understand the role of the company and the role of your institution's IT security staff.
- Ask about retroactive coverage. Since breaches may go undiscovered for some time before a claim is made, you may want to ask for a retroactive date that is earlier than the inception date.
- Discuss how state laws and self-insurance guidelines may mesh with a new cyber insurance policy.
- Perform a cost-benefit analysis with the CFO and other stakeholders.

Costs

The calculation of your potential risk exposure can help determine the coverage you need. For example, if you determine you have 10,000 records that contain PII or PHI and the cost to recover from their exposure is $200 per record, you may want to consider $2 million worth of coverage.

General Coverage Categories[1]

First-party coverage can include the damages directly associated with intellectual property theft, data loss and destruction, hacking, and denial-of-service attacks, including the immediate technical and forensic expenses associated with detecting the breach and its source.

Third-party coverage can include public relations services to coordinate outreach to affected customers and mitigate fallout in the broader community, legal expenses arising from lawsuits brought by customers or third-party businesses, credit-monitoring and fraud-resolution services for the affected individuals and companies, and the associated penalties and fines imposed by domestic and international regulations.

Five-Step Approach to Purchasing Cyber Liability Insurance (Gartner, September 2014)

Additional Resources

- URMIA Survey Shows Members Increasingly Maintain Cyber Liability Insurance, March 2015
- Do I Need Cyber Security Insurance? (video), February 2015
- Five Tips for Companies Considering Cyber Insurance, Gartner, March 2015
- Cyber 101: Obtaining Cyber Insurance—The Process, Woodruff, Sawyer, & Company, April 2014
- Cyber Risks: The Growing Threat, Insurance Information Institute, June 2014

Sustain and Improve Your Information Security Program

The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. The HEISC *Information Security Guide*, created *by* practitioners *for* practitioners, features toolkits, case studies, effective practices, and recommendations to help jump-start campus information security initiatives. Don't reinvent the wheel—get the guide at **educause.edu/security**.

[1] Edward R. McNicholas, Cybersecurity Insurance to Mitigate Cyber-Risks and SEC Disclosure Obligations, *Bloomberg BNA*, August 27, 2013.