Understanding Cyber Insurance

EDUCAUSE Live! Webinar
June 14, 2018

This event is brought to you in partnership with the University Risk Management and Insurance Association (URMIA).

Today’s Speakers

▪ Courtney Davis Curtis
  University of Chicago

▪ Brian Kelly
  Quinnipiac University

▪ Robert Parisi
  Marsh LLC
Agenda

1. What is cyber insurance?
2. Procuring cyber insurance
3. Governance
4. Operationalizing cyber insurance within your information security program
5. What happens if there is a breach?
6. Q&A

What Are Cyber Risks?

Risk caused by:
- Using technology in your operations
- Handling, collecting, storing confidential information
What Is Cyber Insurance?

- **Crisis Management and Event Response Expenses:** Expenses incurred in responding to a cyber event, including retaining forensic investigator, crisis management firm and law firm. Includes expenses to comply with privacy regulations, such as communication to impacted individuals and appropriate remedial offerings like credit monitoring or identity theft insurance.
  
  **NOTE:** Some carriers offer elements of the Crisis Management & Event Response Expenses as a service bundled with the insurance coverage—but not eroding the policy’s limits.

- **Network Security Liability:** Liability to a third party as a result of a failure of your network security

- **Privacy Liability:** Liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.

What Is Cyber Insurance?

- **Regulatory Investigation Defense:** Coverage for legal expenses associated with representation in connection with a regulatory investigation, including indemnification of fines & penalties where insurable.

- **Network Business Interruption:** Reimbursement of your loss of income and / or extra expense resulting from an interruption or suspension of your operations caused by a failure of technology. Includes coverage for business interruption caused by a vendor’s failure

- **Data Asset Protection:** Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.

- **Cyber Extortion:** Ransom or investigative expenses associated with a threat directed at you that would cause a covered loss or claim.
Poll Question 1

Do you understand your cyber insurance program well enough to articulate it to others?

- Yes
- No
- Maybe
- We currently do not have a cyber insurance policy
Understanding Your Cyber Insurance

- Understand the unique exposures and associated risk.
- Be knowledgeable about the cyber insurance program so that program can be articulated to others.
- Prepare for responses to coverage inquires by leadership, including at the board level.
- Increasingly, cyber insurance becomes of a point of negotiation within contracts.
- Consider, what, if any, resources your insurer provides beyond insurance coverage.

Poll Question 2

Do you engage your IT leadership in the cyber insurance renewal process?
- Yes
- No
- Unsure
Procurement and Governance

- Select an experienced broker with expertise in cyber insurance.
- Engage IT leadership given the complexity of the applications questions.
- Allow ample time for the insurance renewal process for the execution of the application.
- Advocate on IT’s behalf.
- Participate with your broker, including with IT, in discussions with the insurer.

Procurement and Governance

- Provide a comprehensive overview on the renewal outcome, especially where decisions are to be made.
- Invite feedback from IT and use benchmarking tools when assessing limits and coverage.
- Share wins with IT.
- Explore methods to allocate the costs of the program to key departments and units.
- Find opportunities for lessons learned, and risk identification from the renewal process. *May result in premium savings or coverage enhancements.*
Poll Question 3

Is your institution taking advantage of the pre-breach services that may be offered by the cyber insurance policy?

- Yes
- No
- Not sure
- We currently do not have a cyber insurance policy

How to Operationalize Cyber Insurance within Your InfoSec Program

- We typically think of insurance after something “bad” has happened.
- With cyber insurance, we think breach or compromise.
- Incorporate post-breach services into your pre-breach planning (coaching, awareness & training, etc.) and coordinating communications with post-breach service providers.
Cyber Policies Can Help Plan Response Actions

They should include the following functions/capabilities:
▪ External cyber attorney/legal support.
▪ Cyber technical/forensic analysis support.
▪ Cyber governance and policy support.
▪ Strategic communications and media support (including call center support).
▪ Identity/credit monitoring.

Breach Coach

Coaches help you prepare for a game, and our there during the game to guide you.
▪ What kind of data do you have?
▪ Where do you keep it?
▪ Who has access to it?
▪ How are you securing it?
▪ When do you purge/delete it?
Awareness Resources

- Newsletters
- Online training and education tools
  - Role-based training
  - Cybersecurity literacy videos
- Posters
- Tip of the Day content

Cyber Insurance as a Force Multiplier

- Many of us have limited staff and budgets
- Cyber policies include technical & forensic support
- Online Readiness Assessments
- Cybersecurity Professional Consultation
- Governance and Policy Support
**Poll Question 4**

Have you experienced a breach?
- Yes
- No
- Unsure

---

**Simplified Data Breach Timeline**
When a Breach Happens

- Immediately notify broker and insure.
- Identify the scope and scale of the breach.
  - What may be comprised? Who may be impacted?
- Engage necessary internal and external parties for assistance.
  - E.g., for the purposes of IT, Legal, Forensic, Notification, Monitoring

When a Breach Happens

- Duties are imposed state, federal, international, and other laws and regulations which may require notification by specified times.
- Evaluate how to prevent future occurrences, including how to be better prepared.
Resources

- Cyber Liability Insurance FAQ
- The Value and Limits of Cyber Insurance
- EDUCAUSE Library: Cyber Insurance

Questions?