FOLEY HOAG LLP

The Role of Cyber Insurance: Protecting Your Company and Avoiding Potential Pitfalls

Cyber Risks And The Boardroom

April 21, 2015

Colin J. Zick
Co-Chair, Data Privacy and Security Practice Group
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com

FOLEY HOAG LLP

Overview

- What is the current data privacy and security landscape?
- Who has cyber insurance?
- Who needs it?
- Is insurance alone enough?

2014 Was A Busy (and Dangerous) Year

- Breaches and cyber attacks have continued at a high frequency.
- While some attacks are very high tech, low tech attacks are very popular and often successful.
- Perpetrators know this and exploit human weaknesses.
- A high percentage of the known breaches/attacks could have been prevented.
- Cyber-espionage is an now established competitive tool.
- The first quarter of 2015 suggests that we are in for more of the same this year and beyond.

Regulators, Company Boards, Accountants and Lawyers Are Focusing on Cyber-Security

- Boards of Directors are recognizing their responsibility and asking more difficult questions to CEOs and CIOs/CISOs.
- Some companies are considering a "cyber-seat" on the Board, or specialized board advisors.
- M&A requires a cyber-security assessment of companies for potential investments.
- FTC, SEC, DHS, HHS and other regulators are recognizing the centrality of cyber and information security to the integrity of our financial infrastructure, and that executives may be held personally responsible.
- Companies are receiving significant penalties from the FTC for cyber-security incidents (fines + 20 year audit requirement).
- Privacy class actions have proliferated.

FOLEY HOAG LLP

Breach Insurance

- Still a developing area
- Limited history of evaluating risk, so policies and premiums can vary substantially
- Scope of coverages also can vary widely depending on the nature of the policy and business
- What can be covered?
  - –Crisis management services
  - –Notification of impacted parties
  - –Credit/public records/fraud monitoring
  - –Fraud remediation services

FOLEY HOAG LLP

Key Cyber Insurance Considerations

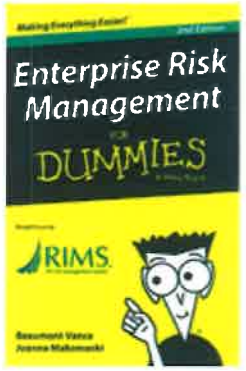
- Policy limits
- Third party coverages
- Premium
- Retention
- Retroactivity
- Coverage for crisis management and breach response
- Provision of counsel/breach coaches

FOLEY HOAG LLP

A Cyber Insurance Quote

LIMIT OF LIABILITY		$5,000,000 Per Claim and in the Aggregate			
COVERAGE SUMMARY					
COVERAGE SECTION		SUBLIMIT OF LIABILITY	RETENTION	RETROACTIVE DATE	CONTINUITY DATE
S&P	Security and Privacy Liability Insurance	$5,000,000	$100,000	For Security Failures:	For Security Failures:
				Full Prior Acts	Policy Inception
	Regulatory Action Sublimit of Liability	$1,000,000		For Privacy Events:	For Privacy Events:
				Full Prior Acts	Policy Inception
Media	Media Content	$5,000,000	$100,000	Full Prior Acts	Policy Inception
NI	Network Interruption Insurance	$5,000,000	$100,000	Not Applicable	Policy Inception
	Waiting Hours Period	8 hours			
EM	Event Management Insurance	$2,000,000	$250,000	Not Applicable	Policy Inception
	Coinsurance	NA			
Premium:				$46,553	

The Role Of Enterprise Risk Management



- What is enterprise risk management?
- Which risks should your company assume, pass or share?
- Where does cyber risk sit among competing risk management interests that corporate leaders must balance?
- How does this relate to existing risks, like business continuity planning?
- Carriers usually count the presence of an ERM program as a factor in favor of providing cyber risk coverage and in providing favorable rates for that coverage.

FOLEY HOAG LLP

A Case Study

- The CISO advised management that the company has maintained cybersecurity insurance since 2008 and that CISO considers it to be the cyber equivalent to a catastrophic health plan – in short, it provides limited coverage with a large deductible.
- In response to a question from a risk manager, he advised that he's fairly isolated from the financial side of insurance and that his only interaction with the insurer in that respect is to "answer their annual [information security] questionnaire."
- While the CISO stated that the company's risk transfer needs are being met by its existing policies – especially when it came to getting the incident response firm on-site quickly – the CISO identified several gaps that he would like to see the broader cybersecurity insurance market fill:
  - Identity theft insurance for breach notification recipients, so individuals who experience fraud and related losses as a result of a breach can be made whole;
  - Elimination of exceptions for widespread incidents such as Internet worms and viruses; and
  - Coverage that applies to data regardless of where it "lives" – for example, beyond the company's network to BYOD devices and cloud/SaaS Services.

Source:
http://www.dhs.gov/sites/default/files/publications/February%202014%20Cyber%20Insurance%20Health%20Care%20Use%20Case%20Roundtable.pdf

FOLEY HOAG LLP

Colin Zick

Partner, Co-Chair, Privacy & Data Security Practice

Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275