CYBER INSURANCE PLAYS GROWING ROLE AS DATA BREACH COSTS SPIRAL

KEY ISSUE:

Data breach costs are becoming increasingly managed through insurance policies, which have their own impact on security programs.

Cyber insurance plays an important role in both managing risk before breaches happen, as well as reducing the significant costs that result from those breaches. Cyber crime costs the global economy more than $445 billion per year[1] at an average of $5.85 million per breach, according to a 2014 study by the Ponemon Institute[2].

- Retailer Target expects insurance to cover $90 million of the $264 million of costs related to its 2013 attack.[3]
- Home Depot said it expects $100 million in insurance payments toward $232 million in expenses from its 2014 breach. [4]
- Anthem Inc. expects its cyber insurance will not be sufficient to cover all claims and liabilities related its 2015 breach, with costs expected to top $100 million. [5]

CHALLENGES AND OPPORTUNITIES:

The growing cyber insurance market can influence the way companies look at their cyber security programs.

The $2 billion market for cyber insurance is **growing rapidly**, and could reach $7.5 billion in annual premiums by 2020. [6] Rates of adoption are highest for healthcare (50 percent), education (32 percent) and hospitality and gaming (26 percent), while 21 percent of utilities and financial institutions, and 18 percent of retail businesses are cyber insured. [7]

In order to obtain a policy, **many insurers call for a strict review of existing security policies and other elements of the security program and then base coverage terms on the results.** AIG, for example, offers policies up to $75 million, but only for organzations like top global banks that are adept at mitigating cyber risk. Ace Group will provide up to $100 million in coverage, but only after an intensive review of clients' security practices. [8]

These reviews will probably get more rigorous as insurance companies pay out more on policies, forcing security and risk management teams to do more stringent reviews and mature their approach to risk overall.

Claims paid out last year to companies that were able to obtain insurance averaged $733,000; large companies (more than $2 billion in yearly revenue) saw average payouts of more than $6 million.[9] Eighty-four percent of claims last year were from companies with revenues under $2 billion.

Average payouts covered three areas:

- **Crisis services** - $427,000 (up to $10 million)
- **Legal defense and settlement** - $1.1 million (up to $6.5 million)
- **Regulatory defense and action** – $2 million (up to $7.5 million)[10]

Encouragingly, security leaders are not broadly observed to be assuming more risk once their losses are insured, probably due in some part to the reviews by insurance companies. Rarely if ever do company executives choose to insure against loss as an alternative to putting in security controls, according to Christine Marciano, president of Cyber Data Risk Managers. [11]

THE PATH FORWARD:

Assess the role of cyber security insurance in overall breach preparedness planning.

Test your assumptions, determine needs and the prerequisites for obtaining cyber insurance, and use this opportunity to improve the overall security program.

Start the process by testing your expectations about cyber security insurance, to make sure you have an accurate understanding of what cyber security insurance can and cannot do.

Challenge assumptions, including these common **misconceptions:**

- I am too small to be a target.
- My general commercial insurance policy will cover a cyber loss.
- The cost is too high.
- Coverage is insufficient.
- Insurance replaces good security practice.

Next, determine the enterprise's cyber insurance needs by estimating the potential impact of the type of incident the insurance is meant to cover. Also, find out what is required in order to obtain coverage.

These questions can help guide your analysis:

- If a breach were to occur, what quantifiable direct impact would it have on business, customers and the supply chain?
- Is there an established framework the insurance provider uses to assess security readiness?
- What does the provider expect you to do to qualify for a suitable policy?
- Will they be satisfied with documentation you provide, or will they require a thorough audit of policies and practices?

Take this opportunity to reassess your overall security, especially if your insurance company requires demonstrated adherence to a given standard or a specific set of requirements.

Cyber security insurance encourages a broader discussion on overall security.

Discussions around cyber security insurance provide a unique opportunity to engage a variety of stakeholders, including finance, operations and risk management to reduce cost and manage risk. While the insurance companies struggle to understand the real risks and costs, they are looking to various "standards" to help quantify risk and assess security postures. During this period in the insurance market's maturity, expect to find that each insurance company may use different benchmarks.

Engage in a dialog with the insurance company and assess whether their requirements are helpful in improving security, or simply require additional unnecessary work that does not lead to enhanced security. When the insurance company and the business are aligned in terms of risk assessment, cyber security insurance can both reduce eventual costs, and serve as a driver for improving your overall security posture.

[1]"Net Losses: Estimating the Global Cost of Cybercrime." June 2014. Center for Strategic and International Studies. Retrieved from: http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf

[2]Multiple sources, including "Global Report on the Cost of Cyber Crime." October 30, 2014. Ponemon. Retrieved from: http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime

[3]Target annual report 2014. March 13, 2015. Retrieved from: http://www.sec.gov/Archives/edgar/data/27419/000002741915000012/tgt-20150131x10k.htm.

[4]Home Depot annual report 2014. February 24, 2015. Retrieved from: http://www.homedepotar.com/assets/pdfs/home-depot-2015-10K.pdf

[5]Anthem quarterly report April 14 2015. Retrieved from: http://www.sec.gov/Archives/edgar/data/1156039/000115603915000006/antm-20150331x10q.htm

[6]"Cyber insurance to triple to $7.5 billion by 2020, attracting disruptors: report." September 13, 2015. PWC. Retrieved from: http://www.reuters.com/article/2015/09/13/us-cyber-insurance-survey-idUSKCN0RD0XO20150913

[7]Beshar, Peter J. "Testimony of Peter J. Beshar, Executive Vice President and General Counsel, Marsh and McLennan Companies, Before the United States Senate Committee on Homeland Security & Governmental Affairs." January 28, 2015. Retrieved from: http://www.hsgac.senate.gov/download/?id=66858569-4eed-4204-8532-919c752cef4e

[8]Finkle, Jim. "Cyber insurance premiums rocket after high-profile attacs." October 12, 2015. Retrieved from: http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012#DoXGMCSxXuD750zf.97

[9]NetDiligence Cyber Claims Study 2014. 2014. NetDiligence. Retrieved from: http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf

[10]Marsciano, Christine "The inside scoop on cyber liability insurance", April 2013. Retrieved from: https://securityintelligence.com/tips-for-implementing-security-behavioral-analytics/

[11]Westervelt, Robert. "Cyberinsurance Policy Sales: Who's Buying?" January 21, 2014. CRN. Retrieved from: http://www.crn.com/news/security/240165498/cyberinsurance-policy-sales-whos-buying.htm

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

12.15 | F1