Bloomberg BNA

Corporate Law & Accountability Report™

DATA BREACHES

Companies, Through Best Practices, Can Help Keep Cyber Insurance Prices Reasonable

BY ROBERT SHAPIRO AND SCOTT SHINE

In speaking to a cybersecurity conference in 2012, then FBI Director Robert Mueller told attendees that there are only two types of companies: those that have been hacked and those that will be. Sadly, with each passing day, those words seem more prophetic. As anyone who follows the news knows, even the federal government has not been immune from being hacked.

Robert Shapiro is of counsel in the Washington, D.C., office of Carlton Fields Jorden Burt and his background encompasses the full spectrum of the insurance industry. He counsels in the regulatory requirements for property and casualty insurers and various types of life and annuity insurance products. He has also assisted in the formation of some of the largest insurance companies in the world and in numerous merger and acquisition transactions involving insurance companies and insurance producer firms.

Scott Shine is an associate at the firm's Washington, D.C., office, counseling a variety of clients, including life insurance companies and private equity firms, on transactional, regulatory and compliance matters.

The list of large commercial companies that have been hacked reads like a who's who of the business world. Companies such as Target, Anthem, Adobe Systems, Inc., Home Depot and Sony have suffered major cyber-attacks on personal data held by each company. Corporate counsel have also reported that they expect the next wave of class action lawsuits to be in data privacy due to increased hacker activity, more frequent internal protocol and security lapses and ongoing consumer and business sensitivity regarding data sharing and use.[1] It is becoming more evident that cybersecurity breaches have emerged as one of the preeminent threats to commercial companies.

These attacks, as well as inadvertent breaches of security by a firm's own employees, inevitably lead to millions of dollars of expenses in rectifying the breach and/or litigation costs from those whose personal information has been compromised. It is estimated that cybersecurity attacks now cost businesses more than $400 billion per year with the average cost to a firm up 96 percent from five years ago.[2]

As the risk and costs associated with cybersecurity attacks have rapidly grown, so too has the demand for cybersecurity insurance. While insurers currently collect approximately $2 billion per year in cyber insurance premiums, some insurance experts expect such premiums will grow to more than $20 billion over the next decade. The anticipated growth is not surprising given that, according to some estimates, a large commercial enterprise should have as much as $100 million of cybersecurity insurance. This is easily understood when one considers the lawsuits alone stemming from these cybersecurity breaches. For example, Target, which was hacked in 2013, has incurred a gross expense of nearly $200 million thus far.

[1] *The 2015 Carlton Fields Jorden Burt Class Action Survey*, available at http://ClassActionSurvey.com/).

[2] Ponemon Institute Survey of 59 firms responding to cybersecurity attacks in 2014 (these figures do not include litigation stemming from such breaches as well as the damage to a firm's reputation) (13 CARE 1020, 5/15/15).

 ISSN 2330-6300

Although the demand for cybersecurity insurance continues to grow, the high price for such coverage continues to be a limiting factor due to insurers' hesitation to commit significant capital to these risks. Insurers' reluctance to commit capital to covering cybersecurity risks doesn't stem from the industry's undercapitalization. Rather, insurers don't have enough loss information from cybersecurity risks to be able to build accurate pricing models.

Keeping up with surging demand for cybersecurity insurance will require an increasing commitment of capital either from existing insurers or from new insurers. The need for additional capacity comes at an opportune time, as the reinsurance market is awash in a sea of capital. This excess capital was intended to reinsure direct writers of insurance, and it is likely that the direct writers will be more willing to increase availability of coverage if they know they can reduce and diversify their exposure through reinsurance.

The reinsurance industry has excess capital due to relatively recent entrants into the market. This capital, often provided by hedge funds and commonly referred to as alternative capital, entered the reinsurance market in search of higher and non-correlated returns than could be achieved by traditional investments such as in the stock and bond markets.

The result of this new money has been to drive down prices for traditional insurance as well as for reinsurance. Although alternative capital initially entered the market mainly to cover property catastrophe risks, such as those resulting from hurricane and earthquake risks, with few natural catastrophes in recent years and interest rates continuing to remain very low, the alternative capital is looking for new markets in which to invest.

Despite available capital within the insurance and reinsurance industry to meet the demands for increased cybersecurity insurance, there is very little loss experience to help insurers quantify potential losses and set rates. This has been a significant contributing factor to the resulting high prices. In turn, the high prices for cybersecurity policies are viewed as cost-prohibitive for many companies that would otherwise seek coverage. For example, after staying flat in 2014, average insurance rates for retailers rose nearly 32 percent in the first half of 2015, according to Marsh & McLennan.

This means there are opportunities for insurers and reinsurers willing to enter the cybersecurity insurance market as well as for those seeking to transfer a portion of the risk and cost of a cybersecurity breach, if insurers can feel comfortable that they can price the risks they are assuming. If this occurs, more capital will flow to insure and reinsure these risks, and more reasonable prices for cybersecurity insurance should result.

What Role Should an In-House Legal Department Play in Obtaining Cybersecurity Insurance?

To help incentivize insurers to devote more capital to this type of coverage, businesses can engage in a number of best practices that will protect the company in the event of a cybersecurity breach and make underwriting as well as pricing easier and thus coverage more available and affordable.

Businesses need to understand their cybersecurity risk exposure and vulnerabilities before seeking insurance, as insurance is not a substitute for taking all reasonable steps to prevent or mitigate damages from such attacks. Accordingly, it is extremely important for a legal department to do a regular assessment to ensure they have adequate security policies and procedures in place and whether, in the event they are hacked, they have the requisite people and authorities correctly prioritized to contain any damage that the organization might suffer from the security breach.

One approach becoming more popular, in addition to utilizing third-party IT specialists, is for companies to hire an independent law firm to perform an assessment of the company's legal policies and procedures related to cybersecurity as well as its rapid-response plan. The risk assessment should help to generate an accurate estimation of the company's cybersecurity readiness. Such assessment should analyze the sufficiency of the company's practices both before and after a cybersecurity incident and should be tailored to the specific company and industry as general best practices for one industry may not be best practices for another type of business. The report based on the assessment should be addressed to the Board of Directors and the Board should have at least one member knowledgeable and conversant in cybersecurity who can critically review it. This will enable the Board to better understand the technical issues involved in minimizing cybersecurity risks, and it will show potential litigants that the Board treated cybersecurity risks as a priority should litigation follow a breach.

"Being mindful of the developing regulatory standards will not only help businesses to establish and maintain updated best practices, it will also allow insurance underwriters to determine whether a potential insured is adhering to best practices that the company's Board adopted."

As part of the assessment, the firm should also undertake an analysis of the company's exposure to litigation and regulatory risks based on the type of personal data it may hold and the industry it operates in. Adoption of a set of best practices tailored to the specific industry can be critical if a company suffers a cybersecurity incident and is subsequently sued. Any shareholder derivative lawsuit or putative class action by a customer will, among other things, allege the failure of the hacked business to establish and maintain effective procedures to either eliminate or respond effectively to cyber breaches. It is therefore important for businesses to be mindful of procedures to respond effectively and promptly to any breach.

An independent assessment can also help identify the relevant laws, standards and pronouncements that various federal and state government agencies are beginning to require relating to cybersecurity so that companies can tailor their internal policies to adhere to those standards and avoid further damages, such as regulatory penalties, in the event of a cybersecurity incident.

   ISSN 2330-6300

For example, only last month the SEC settled a complaint with an investment advisory firm for $75,000 for failing to establish required cybersecurity policies in advance of a breach.[3]

Being mindful of the developing regulatory standards will not only help businesses to establish and maintain updated best practices, it will also allow insurance underwriters to determine whether a potential insured is adhering to best practices that the company's Board adopted.

To confirm that any cyber insurance purchased will actually pay covered claims, the company should annually review its policies and procedures to ensure that they are following through on any commitments made in the application for insurance or by the terms of the policy. In one case, which is currently being litigated in the U.S. District Court for the Central District of California, an insurer refused to pay for the settlement of a case brought after health-care information stored on an insured's network servers was breached.[4] The insurer has claimed that the insured failed to ''follow minimum required practices,'' as obligated under the policy.

If businesses show that they are proactively taking steps to help prevent cybersecurity incidents as well as to minimize the cost after a breach occurs, cybersecurity insurance capacity to meet the needs of businesses should expand dramatically in short order. Once insurers and reinsurers begin devoting capital to this relatively new area, prices should reflect this increase in availability.

The Future of Cybersecurity Insurance

The insurance industry can be slow to react to new opportunities and risks, but they do eventually respond. An example of how capital flows to cover risks can be seen from what's happened to property catastrophe insurance. Risks to property, such as homes, from, for example, hurricanes and earthquakes, used to depend on traditional insurance and reinsurance. Once the probability of hurricanes, for example, was modeled, capital from hedge funds and other institutional investors began to flow to the reinsurance industry. Catastrophe bonds, sidecars and other types of insurance-linked securities were created to compete with traditional forms of reinsurance.

Cybersecurity coverage hasn't been high on the list of exposures for which insurers were willing to deploy capital. The business of insurance involves insurers accepting risk for a price. Insurers are in business to make a profit, and if a risk can't be priced, insurers will not cover it. To do otherwise would be to gamble rather than provide insurance. However, as more loss experience with cybersecurity risks becomes known, insurers will continue to allocate more capital, particularly if businesses adopt cybersecurity best practices and there is reinsurance to spread the risk.

---

[3] See Securities and Exchange Commission Press Release 2015-202, Sept. 22, 2015.

[4] *Columbia Casualty Co. v. Cottage Health System*, USDC Case No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).