Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 1 >>> JANUARY 2015

Responding to Today's Data Breach Environment: What U.S. Directors Really Need to Know about Cyber Insurance

By Paul A. Ferrillo, of Weil, Gotshal & Manges LLP, New York, and Christine Marciano, of Cyber Data Risk Managers LLC, Princeton, N.J.

JPMorgan Chase. Community Health Systems. The Home Depot. Kmart. There has been no shortage of data breaches in recent months — with new developments on an almost daily basis. The age of cyber hacktivisim, cyber extortion, and cyber terrorism is here, and it is not going away anytime soon.

Data security issues are no longer just an IT department concern. Indeed, they have become a matter of corporate survival, and therefore companies should incorporate them into enterprise risk management and insurance risk transfer mechanisms, just as they regularly insure other hazards of doing business.

As the number of data breaches has increased, the demand for cyber insurance has likewise dramatically increased more than that for any other insurance product in recent years.

Every U.S. board of directors should be questioning its officers and management as to "whether or not its company should be purchasing cyber insurance to mitigate its cyber risk." If management answers, "Oh, it costs too much," or "Oh, it will never pay off," second opinions should be obtained. Rapidly. Because neither answer is correct.

For some boards of directors and their respective companies, purchasing a comprehensive cyber insurance policy that covers both first-party and third-party costs helps ensure survival when security fails and large expenditures must be made rapidly to get the company back online. For other more sophisticated companies, cyber insurance may be seen as a way to transfer potential balance sheet risk to an insurance mechanism to protect the company and its shareholders from large, insured losses (no different than if a company would purchase catastrophic property-casualty insurance to protect against natural disasters). Post-Enron and Worldcom, no publicly traded U.S. company would ever forego Directors and Officers insurance coverage to protect against the securities law exposures of the company and its officers. Similarly, today, post-Target, Neiman Marcus, Home Depot, SuperValu and scores of other major cyber security breaches, no company in the U.S. should forego buying cyber insurance to protect against the real, ever-present risk of a major cyber attack and the massive costs associated with such a breach.

Today, It's No Longer a Matter of 'If' Data Breaches Can Have a Real Impact on a Company's Bottom Line and Business Performance; It's a Question of 'When'

Following a data breach, significant costs arise from forensic investigations, lawsuits, data breach notification expenses, regulatory investigations, regulatory fines, attorneys and consultants, PR professionals, and remedial measures. In the blink of an eye, these costs can quickly exceed $5 million or even $50 million in the few weeks after a reported cyber breach.[1] Besides these known costs, a company is exposed to intangible costs as well, including damage to brand reputation, loss of productivity, and a negative impact on business performance (such as loss of store foot traffic because consumers are simply afraid of shopping in their stores anymore), in addition to other liabilities, such as board member liability, shareholder lawsuits for cyber security failures, and declines in a company's stock price. Further, recent history has shown that the plaintiffs' bar seems undeterred from filing new consumer/customer driven lawsuits against companies alleging that they failed to adhere to cyber security "best practices."[2]

If Your Company Experienced a Data Breach Today, Would Your Board Be Ready?

When a data breach occurs, directors and C-level executives must be ready with a business continuity and data breach incident response plan to help minimize their company's liability, exposure, and business performance.

Some of the questions directors and C-level executives should ask themselves — and be prepared to answer before and after a data breach — include:

1) What are the company's most critical intellectual property assets and consumer/customer-based informational assets, and how are they currently being protected?

2) Where are these assets stored or located? Internally, at a third-party data center (in the U.S. or overseas), or in a cloud-based environment?

3) What are the company's practices with respect to diligencing the cyber security practices of third-party vendors and suppliers that may have access to the company's servers?

4) Has the company formally adopted a cyber security standard or practice, such as the National Institute of Standards and Technology (NIST) Cyber Framework, or the International Organization for Standardization's information security management standard, ISO 27001, and what mechanism does the company have to document discussions concerning compliance with those standards?

5) What can go wrong during, and what could be the gross financial impact of, a "significant" data breach?

6) Does the company have a "battle-tested" incident response plan that includes a communication strategy with customers, investors, and law enforcement?

7) How — and will — the company's current insurance policies respond to the cyber security threat environment when and wherever the company is hacked?

8) How much cyber insurance can the company purchase?

Reputational Loss after a Data Breach

Besides data, reputation is the most important asset a company possesses, and it is also one of the most difficult to protect. According to an Economist Intelligence Unit Report (the Report), "Reputation: Risk of risks,"[3] companies struggle to categorize and quantify reputational risk. Especially after a data breach happens, given the fact that there is no formal ownership of reputational risk, responsibility is spread among a wide range of business managers. Nonetheless, companies worry about what could happen to their reputations in the event of a data breach, particularly given the inevitable scrutiny from customers and regulators for perceived failures, and they should adhere to minimum standards of service and implementing data protection measures.[4] While a company may not be able to precisely quantify reputational risk, directors are advised to prioritize the various threats against their companies' reputations. According to the Report, understanding how different aspects of an organization's activities impinge on stakeholder perceptions is therefore a vital aspect of protecting a company's reputation. Furthermore, the Report states that there are three distinct tasks to managing reputational risk: establishing an initial reputation; maintaining it through the rough-and-tumble of business operations; and restoring it when it has been damaged.

Coordinating and creating a "reputational risk" team should be an essential task of every company's data breach incident response group. Incurring reputational damage can be fatal, so having a reputational risk team, with the CEO as the team leader, helps to ensure the company's good standing and minimizes reputational damage after a data breach. Once a data breach happens, the reputational risk team must already have a response plan in place to maintain control of its company's reputation. The reputational risk team, along with the CEO, bears the responsibility of acknowledging its company's concern and commitment, while showing that the company is in control of the situation and is working with any relevant authorities to ensure it will not happen again.

While a company may not be able to insure its reputation with a specific coverage limit, cyber insurance helps guard against and minimize reputational damage by offering a communications team that helps assist a company after a crisis happens. The communications team can help complement the company's reputational risk team and provides a panel of experts that can help advise and assist the company in developing a communica-

   ISSN 1473-3579

tions strategy and managing the response to a potentially damaging crisis.

Besides minimizing reputational damage by offering a communications team, cyber insurance also helps cap the company's communications costs following a crisis, which helps fund the reputational risk team's communications plan budget. Cyber insurance provides help with the coverage costs of communications in response to adverse publicity, including television, print, and online advertising, and the costs of waging a social media campaign designed to address adverse publicity, along with the costs associated with helping to monitor the brand perception of the company.

Incorporating Cyber Insurance into Your Data Breach Incident Response Plan Today

Many directors have openly shared that they feel unprepared to address cyber threats because they lack necessary technical skills and do not understand cyber risk. Fortunately, many directors have realized that cyber risk, formerly seen solely as the IT director's problem, is now also their problem, and therefore their responsibility and fiduciary duty to oversee. Today, when a data breach happens, boards and companies are immediately publicly scrutinized, leaving no distinction between a director or an IT executive. That is why it is best for directors and companies to be proactive in exploring how cyber insurance can help manage cyber risk exposures rather than leave the cyber security gap unfunded when security fails. Purchasing appropriate amounts of cyber insurance can play a significant role in protecting a company's bottom line, rather than costing millions of balance sheet dollars that could have been insured with insurance dollars.

Evaluating Cyber Insurance Policies

Once a company is ready to consider purchasing cyber insurance, it is important to carefully evaluate the plethora of cyber insurance policy options from a variety of angles. The types of coverage offered by cyber insurance policies vary dramatically by insurance carrier, so it is best to start by talking to a knowledgeable insurance broker who has experience with cyber insurance policies.

When evaluating and considering the purchase of a cyber insurance policy, there are several important things to consider prior to investing in a policy:

- **Determine how much insurance is needed and how much risk the company can afford to purchase.** Once the need is determined, a company must figure out how much it can afford to pay out of pocket before any cyber insurance claims may be paid. This will help determine the retention or deductible.

- **Review the types of coverage provided.** While cyber insurance policies are not standard policies and vary widely, coverage typically falls into three categories: liability, breach response costs, and fines and penalties. An experienced and knowledgeable cyber insurance broker or insurance coverage attorney can help evaluate coverage options and determine which coverage best suits the company.

- **Know what triggers the policy.** Will the cyber insurance coverage be triggered in the event of a stolen or lost unencrypted laptop or USB flash drive? Loss related to the failure to secure data? Loss related to a breach caused by a negligent employee? Data held in the cloud? What happens if the company experiences a data breach in which public data is exposed?

- **What does the policy exclude?** Because the purpose of purchasing cyber insurance is to cover risk, it is crucial to learn what risks are excluded in the cyber insurance policy the company is considering.

- **What types of data are covered?** Some carriers specify the types of data covered, while others do not. Here are some things to consider: How is sensitive data defined in the specific cyber policy? Are paper records included?

- **What response costs and services are covered in the event of a breach?** Most carriers offer coverage for breach response costs and breach services. A company will want to check to see if the following are covered in the cyber insurance policy: crisis management and breach notifications, credit monitoring, loss of business income, privacy regulatory defense and penalties, computer forensics investigations, and the hiring of a privacy attorney.

- **Find out if it is possible to select vendors and/or counsel.** Often, companies prefer to select their own vendors or counsel, especially if they have a preexisting relationship with these professionals. Companies should find out whether they have a choice or whether they must use the vendors and/or counsel selected by the insurer as part of the cyber insurance coverage.

The Immediate Advantages of Cyber Insurance

Stand-alone cyber insurance offers companies an immediate solution to transfer the associated first- and third-party costs of a data breach, and offers the crisis management expertise and assistance that is crucial when responding to a data breach.

Immediate Advantages of Cyber Insurance Coverages Include:

(Please note: The cyber insurance coverages described below will vary depending on the specific policies and endorsements selected):

- **Customer notification expenses:** Provides coverage for the expenses associated with notifying the affected individuals. Depending on the policy selected, there could also be coverage to set up a call center to handle calls from the notified individuals. Today, customers are very sensitive to how a company notifies them when their sensitive data has been put at harm. This is a crucial part of the data breach incident response, as customers, as well as regulators, will be lin-

ing up with questions about the extent of the breach and the steps that are being taken to minimize the damage that has already been done.

- **Credit/identity theft monitoring:** Provides coverage for expenses incurred to monitor the credit of an affected individual for one year. When a data breach happens, customers are more susceptible to identity and/or medical fraud. Offering customers a one-year credit/identity theft monitoring program helps decrease this exposure.

- **Privacy and security liability:** Provides coverage for the company's liability arising from a security breach. It is not unusual today for a company to find itself named as a defendant in a lawsuit the day a breach is announced. Some examples of liability coverage may include:

  - negligence by the company for failure to follow "best practices" in cyber protection;

  - a violation of a privacy or consumer data protection law;

  - breach of contract (*i.e.,* merchant service agreements in line with Payment Card Industry (PCI) standards, which govern both retailers and retail vendors); and/or

  - regulatory investigations arising from a breach.

- **Business interruption (depending on the policy selected):** Offers coverage for the company's loss of income incurred as the direct result of a cyber peril or a cloud computing provider's systems failure or impairment due to a cyber peril first discovered during the period of the policy.

- **Cyber extortion:** Offers the company coverage if a hacker demands ransom as a condition of not carrying out a cyber threat. With all of the sophisticated malware attacks of late, this coverage is becoming a valuable component. Some examples of extortion threats may include:

  - threatening a hacking attack or installing virus into the company's computer systems;

  - threatening to disseminate, divulge or utilize information contained or once contained in the company's computer systems; or

  - threatening to damage, destroy or alter the company's computer systems.

- **Hacker damage costs:** Offers assistance with the costs incurred to replace or repair the damaged website, intranet, network, computer system, programs, or data.

- **Privacy regulatory defense and penalties:** Offers help with regulatory defense costs. Depending on the policy, and where insurable under state law, there could be coverage for civil penalties and any related expenses arising from regulatory proceedings not related to compensatory awards.

- **Computer forensics investigation:** When a data breach happens, one of the first parties that must be called in is a forensics investigator to determine the extent of the breach, the cause and what types of data were stolen.

- **Data breach coach (or a privacy attorney):** Offers the company assistance with navigating the various state (and, if applicable, international) privacy laws, and determining who needs to notified and when a breach needs to be reported. Also helps with drafting the breach communication documents and notification letters.

How Much Cyber Insurance Coverage Should Companies Buy?

We believe the answer to that question (without being "tongue in cheek") for boards and companies should be "as much as possible." Once a company has identified its cyber risks and is ready to buy a cyber insurance policy, determining how much insurance coverage to buy must be carefully considered. Using industry benchmark data from companies in your industry or sector that may have experienced a data breach, or from sources such as the Ponemon Institute, can help determine the appropriate amount of coverage the company should purchase. But understand that the dataset in cyber insurance land available today (unlike that in other areas of corporate insurance, such as Directors and Officers liability insurance) is very limited and underdeveloped.

Another source of data to be considered can be found in various cyber security white papers. According to one very authoritative study, the 2013 Ponemon study, "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," when asked to predict a company's maximum financial exposure of security exploits and data breaches for the next 24 months, the average estimate was approximately $163 million.[5]

The amount of cyber insurance that a company can purchase will vary depending on a company's financials, industry, operations, and risk exposures. Presently (and depending upon the aforementioned factors), the maximum amount of cyber insurance coverage any one company can likely obtain is approximately $300 million. Today, what makes boards and companies especially vulnerable is the fact that the costs and chances of a data breach occurrence are unknown but rising exponentially, and there is no normal distribution of outcomes on which to base the probabilities of future effects. Cyber attacks certainly can no longer be considered "black swan" events. They are here to stay. Use the data that is available to benchmark cyber security losses, and "aim high." You likely won't be sorry.

Insuring Your Board and Company's Cyber Risk

Cyber insurance is not a "one size fits all" policy, as no two companies are the same; nor should their cyber insurance policies be. Further, no two insurers are the same in responding to cyber-related claims. When a claim occurs, to the extent possible, it is desirable to

   ISSN 1473-3579

have a cyber insurer whose first response is "Yes, it is covered," rather than "No, buzz off." This is why it is very important that companies work with a specialist cyber insurance broker and cyber insurance coverage counsel who can help customize a cyber insurance policy based upon the cyber and data risks each organization faces.

To help a board and company determine the applicable cyber risk exposures and the possible insurance coverages needed, below is a checklist of first- and third-party risk exposures that can be covered through cyber insurance, depending upon the carrier and cyber insurance policy purchased:

First-Party Cyber Risk Exposures

- **Loss or damage to digital assets:** Loss or damage to data or software programs, resulting in costs incurred through restoring, updating, recreating or replacing these assets to the same condition they were in prior to the loss or damage.
- **Business interruption from network downtime:** Interruption, degradation in service, or failure of the network, resulting in loss of income, increased cost of operation and/or costs incurred by mitigating and investigating the loss.
- **Cyber extortion:** Attempts to extort money by threatening to damage or restrict the network, release data obtained from the network, and/or communicate with the customer base under false pretenses to obtain personal information.
- **Theft of money and digital assets:** Direct monetary losses from electronic theft of funds/money from the organization by hacking or other types of cyber crime.

Third-Party Cyber Liability Exposures

- **Security and privacy breaches:** Investigations, defense costs, and civil damages associated with security breaches, transmissions of malicious code, or breaches of third-party or employee privacy rights or confidentiality, including failures by outsourced service providers.
- **Investigation of privacy breach:** Forensics investigations, defense costs, regulatory penalties and fines (may not be insurable in certain states) resulting from an investigation or enforcement action by a regulator as a result of security and privacy liability.
- **Customer notification/PR expenses:** Legal, postage, and advertising expenses where there is a legal or regulatory requirement to notify individuals of a security or privacy breach, including credit monitoring program costs and PR media assistance.
- **Multi-media liability:** Investigations, defense costs and civil damages arising from defamation, breach of privacy, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
- **Loss of third-party data:** Liability for damage to, or corruption/loss of, third-party data or information, including payment of compensation to customers for denial of access, failure of software, data errors and system security failure.
- **Third-party contractual indemnification:** Financial obligations to third parties due to a security or data breach incident.

Evaluating and Knowing Your Cyber Insurance Carrier's Claims-Paying and Claims-Handling Reputation is Crucial

It is crucial that boards inquire whether the cyber insurance carrier their company is considering has a good claims-paying and claims-handling history.

When a cyber/data breach event happens, there should be no doubt or question as to whether or not a cyber insurance claim will be covered. Companies should have full confidence that their cyber insurance carrier will quickly and promptly respond to an incident *in real time* based upon its superb claims-paying and claims-handling history.

Intellectual Property Exclusion in Cyber Insurance Policies

During a recent panel discussion in which we participated, an attendee asked the panel whether or not trade secrets, if stolen, would be covered by a cyber insurance policy.

Cyber insurance does not cover any actual or alleged infringement, use, misappropriation or disclosure of a patent or a trade secret. Some cyber insurance policies, however, will offer coverage for infringement of intellectual property such as infringement of copyrights and trademarks, but not patent infringement or misappropriation of trade secrets. In addition, depending upon the cyber insurance policy, while there could be coverage for theft or an unintentional breach of third-party confidential corporate information — which may include third-party trade secrets or intellectual property — there is no first-party coverage for the insured organization.

While a cyber insurance policy does not offer first-party coverage for the insured company's patents or trade secrets, those seeking coverage have the option of purchasing a stand-alone intellectual property insurance policy.

Cyber Terrorism

Cyber terrorism is a real, imminent threat that affects companies and governments globally. With today's interconnected networks and devices, cyber attacks can happen anywhere and at anytime. Many cyber attacks originate from, or are at the direction of, foreign governments. In recent years, we have seen attacks from hacktivist groups, such as Lulszec and Anonymous, and it is believed that the U.S. government has classified these hacktivist groups as terrorist organizations. This

can further complicate cyber insurance claims, which can be denied in the event such hacktivist groups are classified as terrorist organizations, and are identified as the cause of your company's cyber attack or data breach.

Cyber insurance policy language varies on whether cyber terrorism will be covered or not. Most cyber insurance policies will be silent regarding the origin of a cyber attack. When exploring the purchase of a cyber insurance policy, a company must be vigilant for any terrorism exclusion, as well as acts of war exclusions, in order to determine the scope of available coverage. Some policies are silent on terrorism, while others contain terrorism exclusions, and only a few provide terrorism coverage. It is important to look for any definition of what constitutes a hacker, as it is in the policyholder's favor that the definition is not limited by a detailed and broadly worded description.

Five Things Every Board Needs to Know When Buying Cyber Insurance

1) Identify the company's cyber risks and determine which risks to avoid, accept, mitigate, or transfer through insurance, and obtain a cyber insurance policy that aligns with the board's cyber risk management strategy.

2) While cyber insurance helps offer an extra layer of defense in a company's robust cyber security program, it is not a substitute for managing the company's cyber risk.

3) Don't rely on a Commercial General Liability policy to cover a data breach, as it most likely will not. Standalone cyber insurance policies offer broader coverage and should be explored by every board, along with an evaluation of the sufficiency of the company's Directors and Officers liability insurance program.

4) Work with experienced and knowledgeable cyber insurance brokers and insurance coverage lawyers who specialize in the various cyber insurance coverages and policies to make sure the company gets the best policy that it can. Often, this means boards must bypass their current insurance broker due to that broker's lack of knowledge and experience in cyber insurance.

5) Evaluate and know the cyber insurance carrier's claims-paying and claims-handling history and reputation before purchasing a cyber insurance policy.

Summary

While no director or company can predict if and when a cyber attack or a data breach will happen, cyber insurance helps minimize the damage if the worst should happen. It is this sort of catastrophic expense (unanticipated, yet "lurking in the shadows") that is often overlooked and not incorporated into a company's budget.

With cyber attacks and data breaches rapidly increasing with no end in sight, the associated costs that are incurred when responding to these incidents should be planned for in advance, instead of depleting balance sheet assets that could have been insured for with insurance dollars.

NOTES

[1] See Home Depot Form 8-K, dated September 18, 2014, noting, among other things, "The Company's fiscal 2014 diluted earnings-per-share guidance includes estimates for the cost to investigate the data breach, provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services, all of which are expensed as incurred in a gross amount of approximately $62 million."

[2] See "Supervalu Hit With Lawsuit After Breach," available at http://www.bankinfosecurity.com/supervalu-hit-lawsuit-after-breach-a-7214; "Community Health Systems Faces Lawsuit," available at http://www.databreachtoday.com/community-health-systems-faces-lawsuit-a-7238.

[3] Economist Intelligence Unit Report, "Reputation: Risk of risks," available at http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf. Note that 36 percent of the Report's survey respondents are companies in the financial services sector.

[4] See "Half of Holiday Shoppers Say They'll Avoid Stores That Got Hacked, Survey Finds," available at http://www.huffingtonpost.com/2014/10/20/shoppers-hacked-stores-survey_n_6004306.html.

[5] "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," Ponemon Institute Research Report, August 2013, available at http://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age.

Paul A. Ferrillo is Counsel in the Securities Litigation Practice Group of Weil, Gotshal & Manges LLP, New York. He may be contacted at paul.ferrillo@weil.com.

Christine Marciano is President of Cyber Data Risk Managers LLC, Princeton, N.J. She may be contacted at christine@dataprivacyinsurance.com.

  WDPR ISSN 1473-3579