CUSTOM RISK SOLUTIONS

What Directors and Officers Really Need to Know About Cyber/Privacy Insurance

Adapted from Chapter 11 of "Navigating the Cybersecurity Storm: A Guide for Directors and Officers" by Paul A. Ferrillo

There has been no shortage of data breaches occurring on a daily basis in recent months. The age of nation-state hacks, cyber hactivism, cyber extortion and cyber terrorism is here, and it's not going away anytime soon.

Dealing with data security issues is no longer just an IT department concern. It has become a matter of corporate survival and should be incorporated into enterprise risk management and insurance risk transfer mechanisms, just as other hazards of doing business are regularly insured for (like fire insurance or hurricane coverage). With the increasing number of data breaches, cyber insurance has dramatically increased in demand like no other insurance product in recent years. Every board of directors should be questioning their officers and management on "whether or not their company should be purchasing cyber insurance to mitigate its cyber risk." If the answer from their management is, "oh, it costs too much, or oh, it will never pay off," second opinions should be obtained. Because neither answer is correct.

For some boards of directors and their respective companies, purchasing a comprehensive stand-alone cyber insurance policy that covers both first and third-party costs helps ensure survival of the fittest when security fails and large expenditures must be made rapidly to get the company "back on line." 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, uninsured losses (no different than it would be to purchase catastrophic property-casualty insurance to protect against natural disasters). Post-Enron and Worldcom, no publicly-traded company would ever forego directors and officers insurance coverage to protect against the securities law exposures of the company and its officers. Today, no company should forego buying cyber insurance to protect against the real, ever-present risk of a major cyber attack.

TODAY, IT IS 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?"

As data breaches accumulate, there are significant costs 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 range from $5 million to $50 million dollars in the few weeks after a reported cyber breach.[1] According to the 2015 Ponemon Cost of Data Breach Report, the average cost of responding to a data breach increased 23% in 2014. The cost of responding to a data breach increased to an estimated $217 per record. Besides these costs, a company is exposed to intangible factors, such as brand reputation and damage, loss of productivity and the impact on business performance (such as loss of store "foot traffic" because consumers are simply afraid of shopping in their stores anymore); and other liabilities such as board member liability, shareholder lawsuits for cybersecurity failures and stock price drops. Further, recent weeks and months have shown us that the plaintiffs' bar seems undeterred from the past in filing new customer-driven lawsuits against companies alleging that they failed to adhere to cybersecurity "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 minimize their company's liability. Here are some questions directors and c-level executives should be asking and be prepared to answer before a data breach and before the purchase of cyber insurance, as they are fundamental to both good cyber governance and an effective purchase of cyber insurance:

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 centre (in Canada or overseas), or in a cloud-based environment? If the company's most critical assets are not intellectual property or customer-related information, but are instead hard "infrastructure" assets like computer-controlled mechanical devices, turbines or pipelines, how are these assets being protected from a cyber attack?
3. What is the company's due diligence process with respect to the cybersecurity practices of third-party vendors and suppliers that may have access to the company's servers?
4. Has the company formally adopted a cybersecurity standard or practice in compliance with federal and provincial privacy legislation requirements for organizations and what mechanism does the company have to document discussions concerning compliance with those standards?
5. What can go wrong and what could be the gross financial impact of a "significant" data breach?
6. Does the company have a Chief Information Security Officer? How often does he or she give presentations to the board of directors?
7. Does the company have a "battle-tested" incident response plan that involves all facets of the company (including the board of directors) which includes a communication strategy with customers, investors, and law enforcement?
8. Does the company have an employee training and awareness program which focuses on spearphishing and other issues like malvertising and ransomware?
9. How and will the company's current insurance policies respond in the event of a hack?
10. How much cyber insurance can our company purchase?

REPUTATIONAL LOSS AFTER A DATA BREACH

Besides data, reputation is the most important asset a company possesses, and also one of the most difficult to protect. According to an Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks"[3] of which 36% of the report's survey respondents were companies in the financial services sector, 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 amongst a wide range of business managers. Nonetheless, companies worry about what could happen to their reputation in the event of data breach and they are deemed responsible by customers and regulators for failing to live up to minimum standards of service and data protection.[4] While a company may not be able to precisely quantify reputational risk, board directors are advised to prioritize the various threats against their companies' reputations. According to the Economist Intelligence Unit 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 reputation to begin with, maintaining it through the rough and tumble of business operations, and restoring it when it has been damaged.

While a company may not be able to insure their reputation with a specific coverage limit, stand-alone cybersecurity insurance can help guard and minimize reputational damage by offering a "crisis management" communications team that helps assist a company after a crisis. The communications team can help compliment your company's reputational risk team and provides a panel of experts who can advise and assist the company in developing a communications strategy and manage the response to a potentially damaging crisis.[5]

CUSTOM RISK SOLUTIONS

INCORPORATING CYBER INSURANCE INTO YOUR DATA BREACH INCIDENT RESPONSE PLAN -TODAY

Many directors today have openly shared that they feel unprepared, lack technical skills and do not understand cyber risk. Fortunately, many directors have transitioned their thinking and realized that cyber risk, formerly seen as the IT Director's problem, is now also their problem, responsibility and fiduciary duty to oversee. Today, when a data breach happens, boards and companies are immediately publicly scrutinized. This is why it is best for directors and companies to be proactive today, and explore how cyber insurance can help manage cyber risk exposures rather than leaving the cybersecurity gap unfunded. Purchasing appropriate amounts of cyber insurance can play a significant role in protecting your company's bottom line.

EVALUATING CYBER INSURANCE POLICIES

Once you are ready to explore cyber insurance, it is important to carefully evaluate the plethora of policy options from a variety of angles. The types of coverage vary dramatically by insurance carrier, so it is good to start by talking with 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 you need and how much risk you can afford to retain.
- Review the types of coverage provided. While cyber insurance policies are not standard policies, and vary widely, coverage typically falls into five categories: third party liability coverage, breach response and remediation costs, business interruption costs, and fines and penalties. An experienced and knowledgeable cyber insurance broker can help evaluate your coverage options and determine which coverages your company should have to cover the range of damages, costs and expenses.
- If you are a retailer, understand what coverage the policy provides in case of a data breach if the retailer faces claims for damages.
- Know what triggers the policy. Will your cyber insurance coverage be triggered for 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, but lost or stolen due to a data breach?
- What is excluded in the policy?
- What types of data are covered? Some carriers specify the types of data covered, while others do not. How is sensitive data defined in the specific cyber policy? Are paper records included (e.g. client records left in a dumpster or on the side of the road for the garbage disposal company that "somehow" end up stolen)? Finally, make sure that if you store your information with a third-party cloud services provider, and that provider is breached, your stand-alone cyber insurance policy would provide coverage for claims arising out of the breach.
- What response costs and services are covered in the event of a breach? Most carriers offer coverage for breach response costs and breach services. You will want to check that at minimum, the following is covered in the cyber insurance policy: crisis management and breach notifications, credit monitoring, loss of business income, privacy regulatory defense and penalties, computer forensics investigation, and hiring a privacy attorney.
- Find out if you can select your own vendors or counsel. Often, companies prefer to select their own vendor or counsel, especially if they have a pre-existing relationship with these professionals. If you have never had a breach incident before, find out if your carrier will help select a vendor for you.

CUSTOM RISK SOLUTIONS

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 below mentioned cyber insurance coverages will vary depending on the specific policies and endorsements selected):

- CUSTOMER NOTIFICATION EXPENSES: Provides coverage for the expenses associated with notifying affected individuals and depending on the policy selected, there could also be coverage to set up a call centre to handle calls from notified individuals. Today, customers are very sensitive to how a company notifies them when their sensitive data has been exposed. This is a crucial part of the data breach incident response as customers and regulators will be lining 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 at least 1 year. When a data breach happens, customers are more susceptible to identity and/or medical fraud. A stand-alone cyber insurance policy that offers customers a 1-year credit/identity theft monitoring program should help decrease this potential damage exposure.

- PRIVACY AND SECURITY LIABILITY: Provides coverage for the company's liability arising from a security breach. As we noted above, it's not unusual today for a company to find themselves on the defendant side of a lawsuit the day after the breach is announced. Some general categories of liability coverage may include:

  - Negligence by the company, for failure to follow "best practices" in cyber protection
  - A violation of privacy or consumer data protection law
  - Breach of contract (I.e., merchant service agreements relating to PCI-DSS)
  - Regulatory investigations arising from a breach.

- BUSINESS INTERRUPTION: Depending on the policy selected, this provides 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 as of late, this coverage is becoming a valuable component. Some examples of extortion threats may include:

  - threatening to attack your computer systems with a hack or virus
  - threatening to disseminate, divulge or utilize information contained or once contained in your computer systems
  - threatening to damage, destroy or alter your computer systems.

- HACKER DAMAGE COSTS: Offers the company help 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 and depending on the policy and where insurable by regional 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 was stolen.

- DATA BREACH COACH (AKA "PRIVACY" ATTORNEY): Offers the company help with navigating the various regional (and, if applicable, international) privacy laws and determining who needs to be notified and when a breach needs to be reported, and also helps with drafting the breach communication documents and notification letters.

How much cyber insurance should companies buy?

We believe the answer to that question for boards and companies should be "as much as possible." Once your 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 sources such as the Ponemon Research Institute can help determine the appropriate amount of coverage for your company.

Unless your board and company has experienced a data breach, most companies lack or have limited data on how the financial impact of a security exploit and data breach would affect them. What makes boards and companies especially vulnerable is that the costs and chances of a data breach occurrence are unknown as there is no normal distribution of outcomes on which to base the probabilities of future effects. Cyber attacks come without warning, and directors must do more to anticipate them and prepare for them. This is why companies must prepare and buy cyber insurance now, and purchase as much cyber insurance coverage as can be obtained.

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

FIRST-PARTY CYBER RISK EXPOSURES:

- Loss or damage to digital assets - loss or damage to data or software programs, resulting in cost being incurred in 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 in service or failure of the network, resulting in loss of income, increased cost of operation and/or cost being incurred in mitigating and investigating the loss.

- Cyber extortion - attempt 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 another type of cyber intrusion.

- Customer notification/public relations 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.

CUSTOM RISK SOLUTIONS

THIRD-PARTY CYBER LIABILITY EXPOSURES

- Security and privacy breaches - investigation, defense cost and civil damages associated with security breach, transmission of malicious code, or breach of third-party or employee privacy rights or confidentiality, including failure by outsourced service provider.
- Investigation of privacy breach - forensics investigation, defense cost, regulatory penalties and fines (may not be insurable in certain regions) resulting from an investigation or enforcement action by a regulator as a result of security and privacy liability.
- 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.

Where does our directors and officers (D&O) liability insurance come into play?

This is another good question that we have been hearing a lot recently. A company's D&O insurance does not come into play really in any of the areas we described above. That is for stand-alone cyber insurance coverage. Where the D&O does come into play is if, upon the announcement of the discovery of a major cyber attack, a company's stock drops by 25% and it and the board is subsequently sued in a securities fraud class action. The securities class action would be a claim under the D&O coverage as would a shareholder derivative action (a suit brought on behalf of the company) against the board of directors for failure to properly oversee the cybersecurity policies and procedures of the company. We mention the D&O here only because in today's environment, it is hard to separate the losses associated with a cyber attack into one distinct bucket. As was the case in the Target cyber attack, the breach and loss of data implicated many potential different buckets of losses and insurance.

Five Things Every Board Needs to Know When Buying Cyber Insurance:

1. Identify your 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 your board's cyber risk management strategy.
2. While cyber insurance offers an extra layer of defense in a company's robust cybersecurity program, it is not a substitute for managing your company's cyber risk. However, stand-alone cyber insurance will help provide valuable loss mitigation services, experienced and helpful claims handling services, and help offset some, if not all, of the expenses of a cybersecurity breach.
3. Don't rely on your Commercial General Liability policy or your Property policy to cover a data breach as it most likely will not. Stand-alone 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 your company gets the best policy that it can. Oftentimes, 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 your cyber insurance carrier's claims paying and handling history and reputation before purchasing a cyber insurance policy

CUSTOM RISK SOLUTIONS

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 in the aftermath.

Companies are, generally, not protecting themselves properly against their exposure to costs associated with a data breach. It's an expense 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 costs incurred when responding to these incidents need to be planned for in advance. Otherwise, you risk depleting balance sheet assets.

Today, regulators appear more understanding about data breaches occurring, but when they do happen (and they will), how a company responds to such events is more important than ever. Regulators and affected individuals will be paying close attention to how an incident is being dealt with and how a company responds as well as what is being done to prevent such incidents in the future.

Cyber insurance with data breach response services helps directors and companies proactively prepare for the unknown data breach response costs of tomorrow. Cyber liability is a growing issue for directors and companies globally and it is no longer acceptable to turn a blind eye or be ill-prepared for such a potential large loss. If your company has not yet purchased a cyber insurance policy, it must do so now.

[1] See Home Depot Form 8-K, dated September 18, 2014, noting, among other things, "The Company's fiscal 2014 diluted earnings-pershare 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 "UCLA Health faces lawsuit for privacy breach in recent cyber attack," available at http://dailybruin.com/2015/08/11/ucla-healthfaces-lawsuit-for-privacy-breach-in-recent-cyber-attack/; "Anthem's big data breach is already sparking lawsuits," available at http://fortune.com/2015/02/06/anthems-big-data-breach-is-already-sparking-lawsuits/.

[3] Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks " Link: http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf.

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

[5] See e.g. "Cybersecurity Insurance," available at http://www.dhs.gov/cybersecurity-insurance ("Traditional commercial general liability and property insurance policies typically exclude cyber risks from their terms, leading to the emergence of cybersecurity insurance as a "stand alone" line of coverage. That coverage provides protection against a wide range of cyber incident losses that businesses may suffer directly or cause to others, including costs arising from data destruction and/or theft, extortion demands, hacking, denial of service attacks, crisis management activity related to data breaches, and legal claims for defamation, fraud, and privacy violations.").

Contact Us

SEAN GRAHAM
Client Executive, Vice President

604 484 3707 | sgraham@cmwinsurance.com
cmwinsurance.com