Published on *The National Law Review* https://natlawreview.com

The Amorphous Nature of Cyber Risk: General Counsels Should Look at the Enterprise-wide Impact of a Breach

Article By:

Litigation

In today's hyper-connected age, safeguarding a company against a security breach is an amorphous task. Determined hackers will ultimately find a way around security protocols. When it comes to assessing cyber risks, many general counsel feel their hands are tied – they know their internal clients are exposed to legal liability, but often they do not fully understand the nature and depth of that liability. While the technical aspects alone of a cyberbreach can be daunting for even the most technologically savvy attorneys, security and systems liability is only one aspect a company faces in the wake of a cyberattack. General counsel would benefit from taking a 360-degree look at how their operation, reputation and overall enterprise would be impacted by a breach. The lessons learned from recent case studies, coupled with the recent introduction of new cyberlegislation, offer guidance to the general counsel in creating and implementing best practices.

Recent Lessons: The Cost of a Data Breach Is Not Just Dollars

Recent data breaches at Target, health insurer Anthem and Sony Pictures Entertainment have taught us how a cyberattack can turn into a full-scale corporate crisis. The total cost of any massive data breach is difficult to quantify and often exceeds simple monetary losses.

The cyberattack of Target's point-of-sale (POS) system resulted in the resignation of Target's CEO and CIO, a profit loss of 46 percent, the filing of lawsuits against the company and a downgrade of Target's credit rating by Standard & Poor's. The monetary costs of tackling the emergency were calculated at over $61 million, not including the disruption to the enterprise and the adverse impact on its operations and reputation.

When Wyndham Worldwide was attacked by hackers who stole information from over 619,000 Wyndham customers from the main network of one of its subsidiaries, the regulatory investigation costs exceeded $5 million. Further costs for litigating against the FTC and defending attendant civil litigations and class actions are slated to add another $5 million. Add to that remuneration, remedial cyberdefense measures, FCC fines, SEC filings, business disruption and reputational loss. The data-breached company faces a hefty corporate charge.

New Legislation Encourages Exchange of Cyberthreat Information

Recent new legislation now affords companies, irrespective of size, the ability to more readily and meaningfully address cybersecurity issues through the exchange of information about cyberthreats between the government and the private sector. In mid-April 2015, the House passed two significant pieces of cybersecurity legislation, during what has been called “Cyber Week.” This legislation offers liability protections to companies that share information on cyberthreat indicators on their networks – such as weak or default passwords, outdated software vulnerabilities, or suspicious code – with each other and the federal government. The first bill, the Protecting Cyber Networks Act, Intelligence Committee Bill, H.R. 1560, was passed by the House on April 22, 2015, by a 307-116 vote. The next day, the Homeland Security Committee’s National Cybersecurity Protection Advancement Act, H.R. 1731, passed by a 355-63 vote.

Both bills are aimed at information sharing in order to decrease the significant cyber risks facing the federal government and the private sector. The bills will allow companies to voluntarily share information on cyberthreat indicators, while requiring them to remove any personal data before sending that information to the government. Companies would receive liability protection from certain regulatory actions and fines only if their data undergoes two rounds of data scrubbing of personal information – once by the company before it gives the data to the government and a second round by the government agency that receives the data. Companies would also be protected from liability and would not be subject to private and regulatory actions if they share cyberthreat indicator data in good faith with the government.

Establishing Best Practice in the Emerging Cybersecurity Landscape

When examined on a deeper level, the new legislation appears to be motivated by larger policy issues. The information sharing embodied in the bills allows the federal government to begin amassing an enormous depository of cyberclaims and loss data. This provides the government with the ability to conduct detailed analytics of real-time data to establish more defensive measures against cyberthreats with greater predictability. The implications of the bills’ liability protections could also encourage companies to obtain cyberinsurance policies, allowing the federal government to avoid a repeat of Lehman by transferring huge potential losses from corporate cyberbreaches to the private sector. While the impact of the legislation is uncertain, what is known is that the anticipated increase in information sharing will impact general counsel and introduce a myriad of additional legal issues.

The question then becomes, what is a general counsel to do internally with all this shared information? Best practices would be to invest in prophylactic cybersecurity protocols, in order to minimize post-breach havoc. Mary Beth Borgwing of Standish Risk Management, LLC, an expert in the insurance and risk management industry, suggests that “organizations need to set goals to prioritize adoption of eGRC standards, education of employees and build enterprise-wide metrics for the impact of breach events and potential breach events on their organizations." Being armed with the right arsenal of cyberbreach information in pre-breach cybersecurity preparedness, post-breach oversight and subsequent remediation measures is essential for general counsel. The following guidelines provide suggestions for the prudent general counsel.

Education. General counsel would be sensible to have a basic knowledge of technical language and terms. Without being able to “speak” the right technical language, it is difficult to ask the right questions and adequately inform the company of the relevant risks. General counsel should coordinate with their CIOs to further educate themselves on pertinent cybersecurity issues and ensure aequate access to external cybersecurity expertise where necessary. They also should

advise company management with respect to providing internal education to relevant employees, similar to how companies might educate employees with respect to employment practices. Education is an essential first step in advising the company on its pre-breach role.

Information Sharing and Analysis Centers. In response to the new legislation that promotes information sharing, general counsel should proactively advise their company's management to join an industry-specific Information Sharing and Analysis Center (ISAC). In the wake of the new cyberlegislation, the National Retail Federation announced it is working to create a program for retailers to access information relating to cybersecurity threats identified by retailers, government and law enforcement agencies and partners in the financial services sector. Being part of a wider industry program will help general counsel arm themselves with information to better protect their individual organizations.

Internal Protocols. General counsel should work with their CEOs, CIOs and CPOs to introduce standard operating procedures for cyberbreaches that include protocols for creating an assessment process and how to act on information that is received. Of particular importance is the efficacy of these policies, because once a breach has occurred, potential shareholder plaintiffs may claim that any insufficiencies in these policies and cybersecurity measures were the cause of their losses. These policies should also be periodically evaluated to take into account the company's risk profile, past security threats and other unique issues. General counsel should review cyberpolicies to ensure they are thorough and up-to-date and confirm that company management understands their role in the event of a cyberbreach.

The caveat to be aware of, however, is that these same internal policies relating to cybersecurity could potentially be turned against the company in subsequent litigation. The Target litigation provides a cautionary tale: shareholders claimed the very fact that Target had cybersecurity policies was evidence that the company was aware of the risks of an incident and failed to fulfill their fiduciary duties to prevent a breach. While creating policies is important, it is equally important to ensure company management understands them and has the capabilities to ensure their implementation.

Conduct a Readiness Test. General counsel would be wise to recommend conducting a readiness test or "cyber fire drill," as this can go a long way towards minimizing liability from the fallout of a potential breach. General counsel should advise company management proactively and ensure that a specific cyberincident response plan is in place, has been properly tested and can be implemented swiftly in the event of a cyberbreach. Considerations should be given to whether the company can address a cyberbreach internally or would require the assistance of outside experts and consultants.

Insurance Coverage. With the current high level and high volume of cybersecurity claims, general counsel should familiarize themselves with the cyberinsurance available to companies to assist with the astronomical costs of a data breach. Most traditional insurance products, such as general and professional liability, do not provide sufficient coverage – if any at all – for cyberbreaches, and may even have specific exclusions. Being conversant in stand-alone cyberpolices that specifically cover the firestorm of damages caused by a cyberbreach is essential. Further, cyberpolices vary greatly in the degree to which they cover breach response costs, lost income and operating expenses, fines and penalties, third-party claims, post-breach forensic investigations and legal fees. Some policies will only provide coverage to notify clients/customers if they are legally required to do so, while others will also provide coverage for voluntary notice. Kelly Geary, vice president with Lemme Insurance, explains that the various types of cyberexposures are evolving rapidly. For example, "social engineering fraud" or "human hacking" claims fall into the cracks between a commercial crime policy and a cyberpolicy, resulting in some carriers creating a new specialty product. Interestingly, "it is

being sold as an add-on to commercial crime policies, not cyberpolicies," notes Ms. Geary. Thus, even where the insurance market is striving to keep up with new exposures, "it is crucial for general counsel to stay on top of the changes in policy wording in order to ensure they have the most up-to-date and comprehensive coverage available in the market."

Lastly, it would be prudent to review the company's D&O policies to ensure sufficient coverage to suit the company's unique risk of derivative claims and shareholder class actions incident to a cyberbreach. Ms. Geary suggests that "general counsel should take care to review all their insurance products to ensure they have the most comprehensive insurance coverage available and a full understanding of the extent to which they have uninsured exposure."

Extended Liability. General counsel should understand that the exposure to the enterprise resulting from a cyberbreach extends beyond a failure of the company's systems. How the company responds to a material breach can raise other liability issues, such as the duties regarding disclosure and due care.

Public Statements. The company's post-breach public statements should be carefully crafted. Post-breach disclosures concerning the company's systems and security, the impact of the cyberbreach or the company's lack of oversight can result in securities class actions or derivative lawsuits.

As daunting as protecting companies from cyberbreaches can be, by understanding the unique issues and concerns that arise in this new landscape, the general counsel is better able to protect and inform his company and board. Having a successful internal protocol and working with an industry ISAC can prove to be a significant asset for general counsel.

National Law Review, Volume V, Number 169

Source URL:https://natlawreview.com/article/amorphous-nature-cyber-risk-general-counsels-should-look-enterprise-wide-impact