METROPOLITAN
CORPORATE
COUNSEL®

JULY / AUGUST 2016 WWW.METROCORPCOUNSEL.COM

SPECIAL SECTION: CYBERSECURITY

Directors Should Look Beyond Cyber Insurance

Law enforcement officials seek accountability in data breaches and cyber loss

By Daniel J. Healy / Anderson Kill P.C.

Cyber risks should have directors and officers thinking beyond specialty cyber coverage that covers their companies' first-party losses and third-party liabilities. Just as cyber risks require input from management outside the IT department, the fallout for improperly managing corporate cyber risks reaches the boardroom. Shareholders have filed derivative suits with varying degrees of success. Regulators have made clear that they can and will enforce laws that punish companies, and their top management, for failing to adequately protect against cyber risks. Key protections against these risks lie in identifying, securing and pursuing insurance coverage beyond a cyber policy – mainly via Directors & Officers and Errors & Omissions policies.

Stating the point succinctly, in April 2016 Fitch Ratings Inc. reported:

> D&O-related exposures from cyber events arise through allegations that ineffective or negligent corporate governance and board oversight were contributing factors behind inadequate systems defenses and a breach that led to losses and/or a sharp decline in share value….[1]

Daniel J. Healy
A partner in the Cyber Insurance Recovery Group of Anderson Kill P.C.'s Washington, D.C. office.
dhealy@andersonkill.com

The Cyber World Continues to Evolve

Among the most rapidly evolving types of risks, cybersecurity has garnered much attention recently. The attention is deserved because the risks posed by data breaches, cyberextortion and other cyber-related losses can be financially immense and long-lasting. Corporate response, too, is evolving. Until fairly recently, many corporations compartmentalized such risks within the IT department, as technical issues. The dangers inherent in that approach have become front-page news.

In defining these risks, it is difficult to put a limit on the scope or severity. When you look at the bottom line, the monetary costs from the highly publicized Target breach are staggering: $150 million in initial response costs, $400 million in replacement credit cards, and an estimated $1 billion of ultimate costs. The focus of this article is on the hundreds of lawsuits filed in the wake of such a breach that target management.

Holding Management Liable for Cyber Losses

Continuing with the Target example, seven directors and officers are the focus of post-breach lawsuits, even after two top executives were terminated. Two of the lawsuits are derivative shareholder suits against directors and officers. One alleges:

> The Company's data breach is currently under investigation by the United States Secret Service and the Department of Justice. Moreover, there are currently no less than ***nine*** class action lawsuits filed against Target on behalf of aggrieved customers.[2]

In another highly publicized breach, Wyndham Worldwide Corporation (Wyndham) was the subject of a derivative shareholder lawsuit against its board.[3] In 2008 and 2009, the company failed to detect that it had been hacked repeatedly. The federal district court dismissed that case in October 2014, relying on, among other things, the business judgment rule and lack of bad faith. To get to the point of dismissal, however, the board had to form a committee to conduct a special investigation probing whether a lawsuit was in the corporate entity's best interests, issue a report and move to dismiss. The costs of those steps can be substantial.

Board members may not adequately grasp the full spectrum of their corporate risk.

Regulators Redefine "Victim"

Relatedly, federal agencies in Washington have stepped up their attention to cybersecurity. Among other things, they more routinely investigate not only the criminals who hack into corporate computer systems, but also the hacked corporation, which may have considered itself to be the victim. While this dynamic is not necessarily unique, it has been an unwelcome wake-up call for some corporations that first suffered criminal attack by a hacker and then were subject to regulatory investigations, potential fines and consent decrees.

For example, Wyndham did not fare as well with the Federal Trade Commission (FTC) as it did in its derivative shareholder lawsuit. The FTC sued Wyndham alleging that Wyndham had violated federal law by engaging in unfair and deceptive acts.[4] Wyndham had stated on its website that it took seriously the protection of personally identifiable information, but failed to implement complex user IDs and passwords, firewalls, and network segmentation between the retail hotels and Wyndham's corporate network.[5] Wyndham countered that the FTC lacked authority to sue Wyndham because the FTC had not promulgated regulations applying the consumer protection statute to data security requirements.[6] The district court and the Third Circuit Court of Appeals disagreed, finding Wyndham engaged in unfair and deceptive practices.[7] The same day, the FTC Chairwoman Edith Ramirez issued a press release stating:

> Today's … decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action … when companies fail to take reasonable steps….[8]

That warning, and the 20-year consent decree that Wyndham has entered into,[9] underscore the regulatory focus on management practices.

Other agencies are joining the fray. The Securities and Exchange Commission (SEC) filed its first cybersecurity enforcement action in September 2015 against R.T. Jones, after the investment adviser allegedly failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information of approximately 100,000 individuals.[10] Despite the lack of evidence that the data stolen has led to actual damages suffered by any customer, R.T. Jones was forced to enter a consent order with ongoing compliance requirements and a fine.[11] The allegation was that R.T. Jones' management failed to adopt written protocols to protect its clients' data. Before that proceeding was filed, the SEC had stated:

> [B]oards that choose to ignore, or minimize, the importance of cybersecurity do so at their own peril.[12]

State attorneys general have also filed enforcement actions against corporations that have suffered data breaches. Grounds for these have ranged from alleged delay in notifying persons whose data may have been compromised[13] to substantive violations of law based on the type of information breached.[14] These cases often focus on management decisions.

Controlling the Risks and Potential Liability Flowing from It

D&O liabilities that stem from evolving cybersecurity risks are not necessarily novel. They look and feel much like other liabilities (accounting improprieties, disclosure violations, etc.). If the corporation suffers financial loss and there were management missteps along the way, shareholder and regulatory attention can be expected.

Enterprise-wide management is needed to address the risks, meaning boards need to proactively address the problem and create frameworks for management to implement protocols and standard practices that cross corporate departments and geography. Many regulators issue guidance that raises these very points.[15] Directors and officers who take these steps position themselves to control an inevitable data breach and seek insurance coverage for their losses.

A key feature in any framework to manage cyber risk is insurance coverage. Insurance can fill the gaps created by the evolving nature of the risk and the near certainty that corporations will face the risk in one form or another. Cyber, property and liability policies often address the direct risk of loss. These policies are important for protecting the corporation against out-of-pocket response costs, property losses and liability to others.

In addition, traditional directors and officers coverage (D&O coverage) and errors and omissions coverage (E&O coverage) may provide coverage for cyber-related losses excluded by some policies. These policies cover "wrongful acts" by management or certain employees. It is important that management not be left bare when lawsuits, such as derivative suits, are brought. Regulatory findings often fuel such suits that focus on management.

While becoming familiar with the terms of the insurance policy is seemingly an obvious first step, a surprising number of corporations are not aware of whether their D&O or E&O coverage specifically excludes some or all cyber risks. If there is cyber coverage, many board members do not understand how that coverage works or what triggers it. Whether it is limited to the insured's own wrongful act, excludes certain types of conduct or excludes certain types of liabilities (regulatory fines) can be highly relevant. Board members are often the least technologically savvy persons at a corporation and may not adequately grasp the full spectrum of their corporate risk. Although that may not be entirely their fault, others may seek to hold them entirely liable.

In the current climate, many insurance companies have responded by capping or even eliminating certain cyber-related coverages. Directors and officers should be mindful of sublimits, exclusions and language that seems unclear. Corporations, and their boards, should be prepared to fight for coverage under traditional D&O policies, as well as under other policies. Recent case law suggests that the facts of a breach may be pivotal in a court's finding coverage, even under "traditional" policy language.[16]

Given the relatively unlimited nature of cyber losses, boards should be aware of what coverage has been purchased that provides "Side A only" coverage as well as Side B. Generally, "Side A only" coverage will defend and indemnify individual directors – as opposed to the company itself – without being first eroded by defending and indemnifying the company. It could be of enormous value in a post-data breach scenario.

Unwanted shareholder and regulatory attention is becoming increasingly difficult to avoid, as data breaches have taken center stage in the media. Directors and officers need to prepare for the unfortunate but increasingly likely event that their company will suffer a breach or other cyber loss and that someone will want to hold them liable.

To review the footnotes to this article, visit http://www.metrocorpcounsel.com.