Beyond Cyber Insurance: Protecting Directors & Officers from Cyber Liability

By Daniel J. Healy, Partner, Anderson Kill

Cyber risks should have directors and officers thinking beyond cyber-specific policies that cover their companies. While these policies often cover first-party losses and third-party liabilities, they may include carve outs and exclusions pertaining to fiduciary liability or to directors and officers themselves. 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 in the wake of cyber breaches, 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….[I]

The Cyber World Continues to Evolve

Among the most rapidly evolving types of risks, cyber security has garnered much attention recently. The attention is deserved because the risks posed by data breaches, cyber extortion 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. Looking just 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.

Such high financial risks require high insurance policy limits. If the first-party losses and third-party liability exceeds policy limits – or the limits of a tower of cyber coverage – then there may be no coverage left for directors and officers when the derivative claims are asserted. As many in-house counsel and board members know, D&O policies provide "Side-A" coverage that covers only individual directors and not the company. Such coverage could prove to the most valuable because the companies' losses do not exhaust the coverage for individual directors and officers for any non-indemnified liability.

Management's Potential Liability for Cyber Losses

Continuing 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.[II]

In another highly publicized breach, Wyndham Worldwide Corporation (Wyndham) was the subject of a derivative shareholder lawsuit against its board.[III] In 2008 and 2009, the company failed to detect that it was hacked repeatedly. The federal district court dismissed that case in October 2014, relying among other things on the business judgment rule and lack of bad faith. To obtain 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.

The 'Victim' Becomes the Regulatory Target

Federal agencies in Washington are paying increased attention to cyber breaches. The SEC filed its first proceeding against a hacked financial institution in the Fall of 2015. The proceedings and investigations put a spotlight on hacked corporations, which may have considered themselves victims. The focus is less on the harm suffered by the hacked corporation's customers whose data was compromised and more on whether the hacked corporation's management had taken appropriate precautions to protect against a data breach.

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

[I] *See* Hoffman, Mark A., "Cyber risks, consolidation pose challenges for directors and officers insurers," *Business Insurance* (Apr. 13, 2016).

[II] *Kulla, et al. v. Steinhafel, et al.*, Case. No. 0:14-cv-00203 (USDC D. Minn.)(filed 1/21/2014) (emphasis original). Motions to dismiss the derivative shareholder lawsuits were pending as of the date of this article.

[III] *Palkon, et al. v. Holmes, et al.*, Case No. 2:14-cv-01234 (USDC D.N.J.)(filed 2/25/2014).

continued on page 2

continued from page 1

alleging that Wyndham had violated federal law by engaging in unfair and deceptive acts.[IV] 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. 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. The district court and the Third Circuit Court of Appeals disagreed, finding Wyndham's engaged in unfair and deceptive practices. 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 …. [V]

As noted above, the SEC filed its first cyber-security 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[VI] Despite the lack of evidence that the data stolen has led to actual damages suffered by any customer, R.T. Jones, like Wyndham, was forced to enter a consent order. The proceeding demonstrates the SEC's commitment to its own statement:

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

State attorneys general also proceed against hacked corporations. Grounds for state proceedings include alleged delay in notifying persons whose data may have been compromised and substantive violations of law based on the type of information that as compromised. These cases similarly focus on management decisions.

Controlling the Risks and Potential Liability Flowing from It

D&O liabilities that stem from evolving cyber-security 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 discusses these very points.[VIII] Directors and officers that take these steps position themselves to control an inevitable data breach and seek insurance coverage for their losses.

Key to any framework to manage cyber risk is insurance coverage. The point of insurance is to have financial security if one's framework for controlling the risk fails or does not fully succeed. Given the near certainty that corporations will face data-breach risk, cyber policies have grown popular rapidly. They often address the direct risk of loss and are important for protecting the corporation against out-of-pocket response costs, property losses and liability to others.

But Directors and Officers may need to look to more traditional policies (D&O coverage) and errors and omissions coverage (E&O coverage) even for cyber-related losses. It is essential to analyze what these policies cover and exclude, sometime in language written before cyber-risk existed.

Such policies cover "wrongful acts" by management or certain employees. Directors and officers should confirm that cyber-related losses are not excluded per se. They should further confirm that the definition of "wrongful acts" is broad enough to encompass a data breach, whether due to an external hacker, internal employee conduct or so-called "social engineering."

Missing a seemingly 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. While that may not be entirely their fault, others may seek to hold them entirely liable. In-house counsel often plays the role of educating the board not only in implementing corporate data-security protocols, but also in purchasing insurance coverage.

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. Exclusions relating to employment practices, bodily

continued on page 3

[IV] The saga of Wyndham's lawsuit with the FTC is laid out through three courts: *Federal Trade Comm. v. Wyndham Worldwide Corp., et al.*, Case No. 2:12-cv-01365 (USDC D. Ariz.); *Federal Trade Comm. v. Wyndham Worldwide Corp.*, Case No. 2-13-cv-01887, Opinion and Order dated 4/7/2014 (USDC D.N.J.)(the case was transferred to New Jersey); *Federal Trade Comm. v. Wyndham Worldwide Corp.*, Case No. 14-3514, Opinion dated 8/27/2015 (USCA 3rd Cir.) and, on remand, the ditrict court's Consent Order entered 12/11/2015.

[V] FTC August 24, 2015 Press Release.

[VI] *Matter of R.T. Jones Capital Equities Management, Inc.*, Admin. Proc. File No. 3-16827.

[VII] SEC Commissioner Luis A. Aguilar, June 10, 2014.

[VIII] The SEC states that it will investigate, and provides guidance about certain factors to determine if corporations are performing reasonable mitigation of cyber risks. *See* https://www.sec.gov/spotlight/cybersecurity.shtml Similarly, the NIST issues a "Cybersecurity Framework." See http://www.nist.gov/cyberframework/

continued from page 2

injury and personal/advertising injury should contain exceptions allowing for coverage of data breaches that lead to such harm. Similarly the companies policies should cover losses at least in every geographic area where the company has data, and probably globally, given the reach of the Internet.

Without making sure a policy contains the appropriate language, corporate policyholders risk finding out they have insufficient coverage after a loss. Recent case law suggests that coverage may pivot on the exact language of a policy, even under "traditional" policy language.[IX]

Given the relatively unlimited nature of cyber losses, boards should be aware of what "Side A only" coverage (mentioned above) they have in place. Generally, "Side A only" coverage will defend and indemnify individual directors for non-indemnified losses – as opposed to the company itself – without being first eroded by defending and indemnifying the company. Other provisions prioritizing rights to coverage can be added as well. Getting the prioritizing language right can be of enormous value in a post-data breach scenario.

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. Preparation must include not only a framework to avoid risk, but also securing coverage, including appropriate D&O coverage with language that will not fail the policyholder in the event of a breach.

About the Author: *Daniel J. Healy is a partner at the law firm of Anderson Kill, P.C. He can be reached at dhealy@andersonkill.com or (202) 416-6547.*

[IX] *Travelers Indemnity Co. v. Portal. Healthcare Solutions*, No. 14-1944 (4th Cir. Mar. 24, 2016) (addressing coverage under a liability policy).