ANDERSON KILL
POLICYHOLDER ADVISOR
The Policyholder Law Firm

D&O Coverage in a Cyber World

By Daniel J. Healy

It has become clear that the fallout for improperly managing corporate cyber risks reaches the boardroom. In the wake of data breaches, shareholders have filed derivative suits, regulators have initiated enforcement proceedings, and management has been forced to defend their cyber-risk protocols.

Just in case directors and officers were unsure, in April 2016 Fitch Ratings 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 . . .

As the likelihood of suffering a cyber event has become nearly a given, a key step in responsibly managing cyber risks is identifying, securing and pursuing insurance coverage. A cyber policy alone may not offer adequate protection against shareholder suits. Directors and officers and errors and omissions policies arguably are more likely to provide the chief line of defense against such suits. General liability and cyber liability policies cover losses involving bodily injury, property damage, personal and advertising injury, and possibly damage to intangible property. They may exclude damage from providing services, from professional liability or from the loss of use of tangible property. They may not apply to shareholder derivative suits or investigations of management either. Additionally, they cover the corporation, not the individual directors and officers. Last, general and cyber liability policies may be exhausted before shareholder claims and government investigations are commenced.

The technological nature of cyber exposures has evolved rapidly. The losses stemming from the exposures vary. Cyber extortion seeks money, other hackers seek to steal the data itself, still others seek to destroy a corporation's data or functionality, and more radical hackers have taken over computer systems to vandalize the corporation's property, such as an oil pipeline that spans multiple countries. The monetary risks alone can be immense. The highly publicized Target breach included $150 million in initial response costs, $400 million in replacement credit cards, and an estimated $1 billion of ultimate costs. In many corporate hacking scenarios the corporation moves swiftly from the victim of a hack to the target of lawsuits.

Management should, of course, minimize corporate exposures by implementing enterprise-wide procedures and standards applicable to cyber risks that cross corporate departments and real-world geography. Several federal agencies, including the Securities and Exchange Commission, the National Insti-

* http://www.businessinsurance.com/article/20160413/NEWS06/160419925/cyber-risks-fitch-ratings-chubb-ace-aig-xl-catlin-u-s-directors-and

Daniel J. Healy is a partner in Anderson Kill's Washington, DC, office and represents policyholders seeking insurance coverage. He has obtained insurance coverage for business interruption losses, D&O liabilities, asbestos liabilities, healthcare plans and other losses. As a former Trial Attorney at the Department of Justice, he has extensive experience in courts across the country. Mr. Healy is a member of Anderson Kill's Cyber Insurance Recovery group and speaks and writes about cyber insurance issues.
(202) 416-6547 | **dhealy@andersonkill.com**

tute of Standards and Technology and Federal Trade Commission, have issued guidance for adopting measures. In addition to preventing some breaches, adopting good practices will also position a corporation to minimize loss after the inevitable, successful attack, at which time insurance coverage becomes vital.

Given the variety of losses and liabilities potentially triggered by a data breach, one should not assume that a single liability or cyber policy will provide complete protection. Cyber policies have grown popular rapidly, but given the above-mentioned characteristics of such policies, directors and officers may need to look to more traditional E&O and D&O coverage, even for cyber-related losses.

E&O policies typically cover losses from services provided to clients. D&O policies generally cover "wrongful acts" by management. Of course, cyber-related losses should not be specifically excluded, though they sometimes are. Additionally, the definitions of services, "wrongful acts" and other key grants of coverage should be broad enough to encompass the types of events that could lead to a data breach, whether due to an external hacker, internal employee conduct or so-called "social engineering." A surprising number of corporate managers and their boards are not aware of whether their D&O or E&O coverage specifically exclude cyber risks, and do not understand how cyber coverage works or what triggers it.

Prudent policyholders should carefully review sublimits, exclusions and provisions that seems unclear, such as language defining the scope of exclusions for damage to electronic equipment. Exclusions relating to employment practices, bodily injury and personal/advertising injury ideally should not apply to data breaches that lead to such harm. Similarly, the covered geographic area should include those locations where the company stores data, and perhaps extend globally, given the reach of the internet. Additionally, as many in-house counsel and board members know, D&O policies provide "Side-A only" coverage that should not be eroded by corporate losses. Given the high monetary exposure, it would be unfortunate to have no "Side-A only" coverage for a data breach due to exclusions.

Without making sure a policy contains the appropriate language, directors and officers 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. *The Travelers Indemnity Company of America v. Portal Healthcare Solutions, L.L.C.*, No. 14-1944 (4th Cir. Mar. 24, 2016) (addressing coverage under a liability policy).

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 be mindful of the coverage, or gaps in coverage, their corporation may have. Taking stock now will greatly increase the chances of recovering insurance proceeds when they are needed, after a loss.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estates, Trusts and Tax Services, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA for Client Service and Commercial Awareness, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. Based in New York City, the firm also has offices in Philadelphia, PA, Stamford, CT, Washington, DC, and Newark, NJ.