ANDERSON KILL
POLICYHOLDER

July 2019

ALERT

Mind Your D's and O's (Insurance): Protecting the Board from Executive Cyber Risk

By Dennis J. Nolan

Each week brings a barrage of cyberattack headlines. In late 2018, Marriott announced the theft of almost 500 million customers' personal data. Marriott was not alone — one recent survey suggests that nearly three in five companies were hit by one or more attacks in 2018. Increased regulatory scrutiny and shareholder litigation following cyber events pose a greater threat than ever to a company's reputation and balance sheet. As data breaches grow in scope and cost, officers and directors, who ultimately are responsible for the organization's survival, must emphasize appropriate insurance coverage for themselves.

A Wake-Up Call from Regulators and Shareholders

It is practically given that regulators and angry shareholders will point fingers at senior management following a significant data incident.

A patchwork federal, state and international framework makes navigating the cyber regulatory landscape challenging. Many federal agencies, including the Securities and Exchange Commission, Federal Trade Commission and the National Association of Corporate Directors, publish best practices and set requirements for companies to identify vulnerabilities, secure data, and respond to breaches. In 2018, the SEC issued guidance regarding public company disclosures about material, known cyber risks or uncertainties. A board must fully inform itself and make reasonable decisions about disclosures it ought to make or face liability.

At least 35 states introduced over 250 cyber-related bills in 2018. Notably, the New York Department of Financial Services (DFS) cybersecurity regulations became fully effective in March of this year. DFS-licensed financial institutions must certify implementation of a board-approved written cybersecurity policy; a chief information security officer position responsible for implementing, monitoring, and enforcing the program; various safety controls; and procedures for third-party service providers.

The European Union's General Data Protection Regulation (GDPR) requires certain businesses to designate a data protection officer who must report directly to the highest levels of management, be given adequate resources, and operate independently. It stipulates potentially massive

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue, Suite 2450
Los Angeles, CA 90071
(213) 943-144

www.andersonkill.com

who's who

Dennis J. Nolan, a shareholder in Anderson Kill's New York office, concentrates his practice on insurance recovery. He represents policyholders exclusively in various sectors, including financial services, technology, manufacturing, and retail, with respect to a broad range of insurance policies, including Marine Cargo, Cyber, Directors and Officers, Errors and Omissions, and Commercial General Liability policies. Mr. Nolan also has extensive experience representing debtors and creditors in insurance coverage disputes in complex chapter 11 cases. He co-chairs the firm's marine cargo industry and bankruptcy groups.

dnolan@andersonkill.com
(212) 278-1659

fines for violations — the greater of 20 million euros or 4% of annual worldwide turnover.

Cyber enforcement actions spiked in 2018. The SEC commenced 20 cases, with another 225 ongoing investigations, including its first enforcement action for failure to disclose a breach, issuing a $35 million fine to Yahoo. The FTC brought 29 actions last year, and reportedly has approved a $5 billion settlement with Facebook for numerous privacy missteps.[1] States were more assertive, too. Eight states entered into a consent decree that requires Equifax to perform a detailed assessment of cyberthreats and increase board oversight of cybersecurity. In Europe, meanwhile, while less than a hundred GDPR fines have been levied, it's rumored that Facebook is facing a $1.6 billion GDPR penalty.

Every large data breach can lead to D&O liability in the courtroom, too. Any doubt that the liability tide has changed was removed in December 2018, when a securities class action was filed *the day after* Marriott announced its breach.

Early lawsuits accusing senior management of sanctioning lax cybersecurity were dismissed before any factual hearing. A crack in the dam appeared when Home Depot and Wendy's settled derivative suits, even though those cases never made it past the pleadings stage. Both companies paid nominal attorney's fees and adopted prophylactic measures, including the establishment of a separate board-level committee to oversee cybersecurity. The dam burst when Yahoo settled a securities suit alleging that it falsely represented its cybersecurity practices and failed to timely disclose the breach. This past April, Yahoo boosted its settlement offer to $118 million after the trial court rejected an initial $80 million offer. Yahoo also recently settled a derivative action for $29 million.

These settlements signal that D&O cyber liability has entered new and potentially dangerous territory. Earlier data breach claimants often failed to prove actual economic harm occurred from a breach. Yahoo's breach disclosure caused a $350 million drop in Verizon's acquisition price, and large companies sustaining data breaches are experiencing significant stock drops. Equifax's value dropped 33% in the wake of a massive breach. And this past May, Moody's slashed Equifax's rating to negative, noting that it's "the first time the fallout from a breach has moved the needle enough to contribute to the change."[3] Expect future litigants to point to similar tangible damages to avoid dismissal of their claims.

Considerations When Purchasing Insurance Protection for the Board

Regulators have stated that prudent corporate cyber governance includes insurance protection. At a minimum, coverage is necessary to protect executives, who could be left on their own to face regulators and shareholders. This risk is significant for smaller companies that might lack resources to provide adequate indemnification.

Fortunately, D&O insurance remains one of the broadest liability policies. Public and private D&O forms will respond to assertions

that the board failed to adequately disclose cyber risks, implement or manage proper cyber policies, or respond properly to a data breach.

Given the prevalence, length and expense of regulatory inquiries, make certain that coverage extends to the costs of preliminary investigations and non-formal inquiries, not just formal investigations, and that those costs are not sub-limited.

Keep the policy clear of cyber exclusions. Some policies exclude privacy incidents, which should be carved back for resulting securities claims. While most policies will cover the costs of criminal investigations or proceedings, they will exclude criminal fines or fraud penalties based on public policy. Ensure that the exclusion only applies in the event of a final, non-appealable adjudication.

Relatedly, look out for "intentional misconduct" exclusions; given that most conduct is intentional, limit the exclusion to an intentional "violation of law." The policy also should contain a severability provision, so that one director's misconduct does not impact another's coverage.

Private companies must beware of the "insured versus insured" exclusion. These D&O forms often define "insured" broadly to include advisory boards, committees or employees. If any of these cooperate in a lawsuit against management, the policy will not respond. Remedy this by carving back cyber-related claims or substituting an "entity versus insured" exclusion.

D&O policies should protect directors and officers in cases where corporate indemnification proves problematic. Management cannot be indemnified for payments to resolve derivative suits or for breaches of the duty of loyalty. In some cases the company may refuse to indemnify to the fullest extent of the law. In many D&O policies, a "presumptive indemnification" clause provides that if the company does not indemnify when legally permitted for a reason other than insolvency, then the insured individual must pay the full retention — often millions of dollars for larger companies — before the policy responds. Executives should push to remove this clause, or narrow it to allow executives to access first dollar side-A coverage.

Executives should consider adding a separate side A difference-in-conditions policy to the arsenal. This will bypass presumptive indemnification issues and drop down to allow dollar-one coverage without the required retention. It also provides additional limits when the underlying policy, shared by the company and management, is exhausted. Because it "drops down" to fill underlying coverage gaps, it lacks many of the exclusions seen in primary policies or "follow form" excess policies, and generally only contains an intentional conduct exclusion, subject to a final adjudication. Management can also enjoy broader coverage, including costs for pre-claim inquiries and informal investigations and affirmative coverage for fines and penalties against the individuals.

Retroactive dates can be thorny with derivative or securities class actions. Some cyber incursions can go undetected for months, and a complaint inevitably will include broad allegations that the company failed to implement proper protections or monitor its practices for years. Such vague allegations will span a period of time long before the breach, potentially back to the computer system's implementation. Don't acquiesce to protection from the inception date; instead, seek a retroactive date that predates the policy by several years.

Insurance applications can also be tricky. Misstatements may result in a coverage denial. Some public companies submit corporate disclosures and investor decks, rather than applications. A public filing that misrepresents a company's cyber practices could lead not only to an investor suit, but also to a coverage fight, even if the claim is otherwise covered under the policy's plain terms, on the grounds that material misrepresentations were made when purchasing the policy. Do not allow insurance companies this opportunity. Answer questions intelligently and gather all relevant information from various departments in the organization.[2]

Conclusion

In a technology-driven world, with complex, evolving, and costly cyber risks that resonate in the boardroom, purchasing robust D&O insurance is essential to reduce the sting when regulators and shareholders knock on the boardroom door following a data breach.

ENDNOTES

1 *https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html*

2 *As always, provide notice to insurance companies promptly, and although this article focuses on D&O insurance, policyholders should not forget to review and provide notice under other lines of coverage.*

3 *https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html*