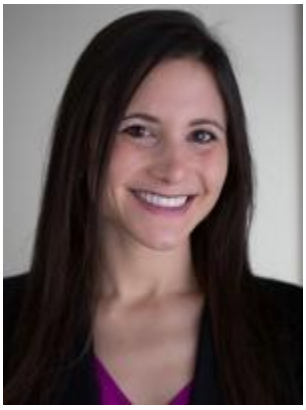
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data Breaches Bring D&O Insurance Issues

Law360, New York (September 9, 2015, 10:11 AM ET) --



Rachel Raphael

As cyberincidents continue to occur with increasing frequency and severity, companies of all sizes have turned a critical eye to the processes they have in place to prevent such incidents and deal with breaches if and when they take place. Historically, companies and corporate boards did not pay as much attention to cybersecurity as other corporate risks. However, the 2014 shareholder derivative suits faced by Target Corp. and Wyndham Worldwide Corp. have officers and directors thinking twice, and reasonably so.

Companies today tend to rely heavily on the digital space to gather and store sensitive and confidential information. Any company that keeps its own information or that of its customers or business partners in an electronic format is at risk.

A recent July 2015 decision by the Seventh Circuit to reinstate a consumer data breach class action against Neiman Marcus should give companies and their directors and officers further cause for concern. In Remijas v. Neiman Marcus Group LLC, No. 14-3122 (7th Cir. 2015), the Seventh Circuit indicated that the bar may be getting lower for class actions based on data breaches. The court concluded that the Neiman Marcus action plaintiffs did not have to wait to become victims of identity theft or fraud before filing suit — they had standing based on the theft of financial information alone. And file they did.

As a result, 2015 and beyond may very well bring mega data breaches that are followed by lawsuits against corporate boards concerning the adequacy of cyberrisk oversight and data breach response procedures.

The expected increase in cyber-related directors and officers litigation likely will also lead to increased cyber-related claims under D&O insurance policies and increased coverage disputes. Although there may be some coverage for these types of losses under D&O insurance policies, the marketplace is developing tailored cyber policies that may provide a more fulsome backstop.

D&O Policy Basics

D&O insurance policies are designed to indemnify a company's directors and officers and/or the company itself for expenses and losses suffered in connection with suits alleging wrongful acts by directors and officers committed in their capacity as directors and officers. For public companies, this

coverage is often confined to securities claims. But for private companies, D&O policies generally contain no such limitation and may provide coverage when claims are brought by nonshareholder plaintiffs such as customers, creditors and suppliers.

Although most policies have the same basic structure, there is no standard policy form for D&O policies like the ISO forms found for commercial general liability policies. As a result, whether and to what extent a D&O policy will cover losses suffered by a company in connection with a data breach will vary based on a policy's specific language. Generally speaking, however, when a data breach occurs, policyholders may be expected to submit claims based on resulting suits under their D&O policies (i.e., securities claims against public companies) when the allegations concern the "wrongful acts" of directors and officers.

D&O Policy Exclusions That May Affect Data Breach Coverage

At this point, specific cyberliability exclusions exist but are not yet mainstream in the D&O market. However, there are more generic D&O policy exclusions that could affect coverage for losses resulting from a data breach:

Regulatory Exclusion

Some D&O policies contain exclusions for claims brought by governmental, quasi-governmental or self-regulatory agencies. This means that if the Federal Trade Commission, for example, brings an enforcement action against a company and/or its directors and officers for failing to maintain proper security measures to protect sensitive consumer information, the D&O policy may not provide coverage related to these claims.

Prior/Pending Litigation Exclusion

Generally, D&O policies exclude coverage for claims that are pending prior to policy inception as well as later claims based on the same or related facts and circumstances. Thus to the extent that a company has been the subject of a claim relating to a data breach before the inception of the D&O policy, claims associated with that earlier breach may not be covered. Even claims related to a second breach that does take place during the D&O policy period may not be covered if this second breach arises from the same or related "facts and circumstances" as a pre-policy claim — perhaps where, for example, the second breach occurs because of the company's failure to improve its security measures after a prior breach.

Bodily Injury Exclusion

D&O policies often exclude coverage "for any actual or alleged bodily injury," and some D&O policies also include within this exclusion a reference to, among other things, a violation of the right to privacy. In certain circumstances, possibly based on the nature of the compromised information, a data breach may constitute a violation of one's right to privacy. Thus where the violation of one's right to privacy is considered "bodily injury" under the terms of the policy, the company and its directors and officers may be unable to seek coverage for related claims.

Contractual Liability Exclusions

A D&O policy may not cover losses that are based on, arising from, related to or a consequence of an

actual or alleged liability that is assumed under a contract or agreement. When a company contracts with a third-party vendor to handle sensitive customer information, that agreement may contain a contractual liability clause that leaves the company exposed. If the third-party vendor does not have sufficient security measures to protect sensitive information, and a data breach occurs, liability assumed by the company via this third-party contract may not be covered by the D&O policy if it contains this exclusion.

Conclusion

Even if a given D&O policy does not specifically exclude losses resulting from a cyberincident, this is no guarantee that such losses are covered. Depending on the nature of the lawsuit, the data compromised, and the specific policy language, significant coverage issues may be implicated by a cyberincident. As the number of cyber-related lawsuits against directors and officers increase, so too may the prevalence of specific cyber exclusions.

Further, even where coverage may potentially exist, a D&O policy will only respond to specific types of claims. D&O policy coverage for public companies is generally limited to securities-based claims such as shareholder class actions and derivative suits. Thus, although a D&O policy may potentially provide some coverage for claims related to a data breach, it is no substitute for a stand-alone cyberinsurance policy.

—By Rachel Raphael and Ellen Farrell, Crowell & Moring LLP

Rachel Raphael is an associate and Ellen Farrell is a senior counsel in Crowell & Moring's Washington, D.C., office.