New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Insurance Law
WWW.NYLJ.COM
MONDAY, DECEMBER 1, 2014

Cyber Liability Insurance: What Coverage Can You Expect?

BY HEIDI LAWSON AND DANNY HARARY

"Cyber liability insurance" is often used to describe a broad range of insurance policies in the same way that the word "cyber" is used to describe a broad range of information security related tools, processes and services.

In the past, coverage for certain cyber risks was sometimes found in already-existing policies, including kidnap and ransom (K&R) and professional liability or errors & omissions (E&O) coverage. Limited coverage has also been available in crime policies if electronic theft is added to the policy. Even where coverage for cyber risks has not been explicitly negotiated, policyholders have recently attempted to secure coverage for cyber breaches under commercial general liability (CGL) policies.[1]

With the seemingly daily reports of data breaches plaguing some of the country's largest retailers and other businesses, insurers have responded by offering an updated form of "stand-alone" cyber liability insurance policies. In contrast to CGL, directors & officers (D&O), and E&O policies, where the terms are largely predictable, these new stand-alone cyber liability policies are not standard, with significant terms and conditions in flux and distinct from policy form to policy form. While insurance coverage for data breaches isn't entirely new, the most recent wave of stand-alone cyber liability policies is gaining more momentum in the marketplace than it has in the past. Generally, this most recent generation of stand-alone cyber liability policies offer both first-party

© BIGSTOCK

HEIDI LAWSON *is a member and* DANNY HARARY *is an associate at Mintz, Levin, Cohn, Ferris, Glovsky and Popeo.*

and third-party coverage for certain cyber-associated risks. These policies typically provide coverage through numerous insuring clauses that afford coverage for losses arising out of data or privacy breaches, such as expenses related to the management of an incident, including the investigation, remediation, notification and credit checking. In addition, these stand-alone cyber policies will usually provide coverage for business interruption losses, extortion, network damage, and regulatory investigation costs arising out of a cyber event.

However, despite the fact that there are many kinds of policies that cover "parts" of a cyber-event, the parts that are not covered are still significant. Unfortunately, brokers and insurers tend to organize their internal business operations around certain insurance products, such as D&O, CGL or E&O, with sometimes very little coordination of coverage between the different lines of business. This fragmented approach to insurance in the market often creates confusion and ambiguity regarding where one policy stops covering a certain risk and another policy starts. There are separate brokers, underwriters and claims adjusters for each kind of policy. As a result, individuals become highly specialized in a particular area and sometimes rarely work with a range of insurance policies. Innovation loses out to specialization.

Cyber liability is a very complex risk that does not neatly fall into any one insurance policy. When a board of directors is faced with a derivative suit for failure to oversee the protection of customer information, there is a risk that their D&O policy will not cover the lawsuit because there is a standard privacy exclusion in all D&O policies. Even if a separate cyber liability policy was purchased, that separate "stand-alone" cyber liability insurance policy will not cover the board of directors, because a stand-alone cyber policy does not cover derivative suits. So, where does that leave the board of directors? Exposed.

An excellent example of this potential exposure is demonstrated by recent derivative lawsuits brought against directors of companies in which cyber breaches have resulted in the theft of customers' personally identifiable information (PII), such as credit card numbers, expiration dates and security codes. Plaintiffs in these cases have charged the defendant directors and officers with breaching their duties of good faith and loyalty to the company by failing to implement adequate safeguards to prevent the breach.[2]

With the seemingly daily reports of data breaches plaguing some of the country's largest retailers and other businesses, insurers have responded by offering an updated form of "stand-alone" cyber liability insurance policies.

Directors named as defendants in derivative lawsuits for cyber breaches face significant liability. The directors, however, may be lulled into a false sense of security, looking to their company and its insurance policies for indemnification. The company, however, likely may not be permitted to indemnify the directors, as corporate indemnification for settlements or judgments in derivative lawsuits is prohibited in Delaware,[3] which sets the corporate indemnification standard. Similarly, the director may not fare well under the company's D&O policy. As we have already noted, such policies often include a standard privacy exclusion, which could be construed as precluding coverage for such a lawsuit. The defendant director will also not be able to recover under the company's stand-alone cyber policy, because these policies, as currently drafted, do not cover director or officer liability. Thus, the unsuspecting director, assuming the availability of several independent sources of indemnification, finds herself exposed to personal liability in a high dollar lawsuit.

Similarly, while a separate stand-alone cyber liability insurance policies cover privacy breaches, those breaches typically must be the theft of PII. However, what about the theft of a hedge fund's trading information? Uncovered.

Another frequent gap in coverage associated with stand-alone policies relates to dispersal of sensitive data through acts of company employees. If the employee's actions are intentional, many policies expressly exclude employee breaches, and otherwise, an insurer may be able to assert that coverage is precluded on account of the conduct exclusion, which typically excludes intentional or dishonest conduct. However, what if the employee's release of the sensitive information (whether belonging to the company or a third-party) is accidental? Many policies only cover the costs associated with the *unauthorized* acquisition or access to PII. In this scenario the employee was authorized. Therefore, the insurer can likely maintain that coverage is simply not triggered because the employee was authorized to access the PII in question.

While the gaps in coverage afforded under a stand-alone cyber policy may be significant, the reason for these gaps has much to do with the difficulty in underwriting this coverage. The difficulty lies in the specificity of risk on a company-by-company basis, as well as the relatively underdeveloped actuarial information pertaining to the broader scope of cyber risks. One reason for this lack of data on cyber risk management stems from the recent traction that insurers are gaining in the market with these newer stand-alone cyber liability policies. Another is the relatively short form questionnaires and applications required by insurers eager to place these policies and gain market share, rather than demanding a detailed analysis of every prospective policyholder's internal cyber risk management protocols.

An intriguing question surrounding stand-alone policies, is how courts in New York, and throughout the nation, will interpret their provisions in the insurer-policyholder battles that are surely on the horizon. As of the date this article is being submitted for publication, the authors are unaware of any published decisions construing these new stand-alone cyber policies. Some would be inclined to assume that the recent novelty and growing popularity of these policies will result in decisional law that favors policyholders over the insurers that drafted the policy terms. New York courts, however, will be forced to construe these policies within the established legal framework guiding

insurance policy interpretation. As a result, the structure of the new stand-alone cyber policies would seem to favor insurers. Unlike other policies, such as D&O policies where the coverage grant is quite broad and narrowed through exclusions, the stand-alone cyber policies contain numerous insuring clauses which in turn are delineated by several layers of defined terms.

The structure of these policies will therefore be critical in the policies' interpretation. For instance, it is axiomatic that in New York, it is the insured's burden to establish coverage in the first instance, and once established, the burden shifts to the insurer to prove that coverage is excluded.[4] Therefore, as an initial general observation, because much of the coverage, as well as coverage limitations, are found in the insuring agreement and definitions, the onus will be on policyholders to prove that coverage is triggered in the first instance. Whereas D&O and E&O coverage can usually be more easily triggered by demonstrating a claim arising out of an alleged error or omission, the new stand-alone cyber policies demand much greater specificity of loss before coverage will be triggered. Thus, for example, it will not suffice for a policyholder to claim coverage for any kind of cyber breach. Instead, most stand-alone cyber liability policies afford coverage only if "Personally Identifiable Information," a defined term, or some variation thereof, is breached. Therefore, the burden is on the policyholder to demonstrate that PII, within the meaning of the policy, was accessed without authorization.

Another critical canon of construction is the rule of ambiguity. "Under New York insurance law, if there is a reasonable basis for a difference of opinion as to the meaning of the policy, then the language at issue is deemed to be ambiguous and thus interpreted in favor of the insured."[5] While the rule of contra proferentem—interpreting contracts against the drafter—is a harsh one, not every difference of opinion gives rise to an ambiguity. "An ambiguous word or phrase is one capable of more than one meaning when viewed objectively by a reasonably intelligent person who has examined the context of the entire integrated agreement and who is cognizant of the customs, practices, usages and terminology as generally understood in the particular trade or business."[6]

The new wave of stand-alone cyber policies leaves the door open for insurers to draft cyber policies from scratch, to correspond to the rise of a new risk that is here to stay. However, given the novelty of the risk and the policies, as evidenced by the absence of any cases construing these policies, insurers should try to inject as much certainty as they can into these new policies. Clearly defined terms and conditions allow the insurer to avoid at least some of the inevitable conflicts that devolve into litigation regarding the meaning of ambiguous wording. Insurers can look to their experience with other policies and policy forms that they have written, like CGL and E&O, to inform the stand-alone policy wording, and to harmonize their policies to the extent possible, which serves the interests of insurers and policyholders alike. There are numerous terms and conditions, and even exclusions that already exist in other policies that have already been interpreted by certain courts and can be utilized in the stand-alone cyber policies to bring as much predictability as possible. It also gives insurers an opportunity to harmonize coverage between various lines of business, giving them a competitive edge and lessening the number of gaps in coverage and unhappy insureds.

Based on the foregoing, it would be unwise for policyholders to view stand-alone cyber liability policies as a panacea for responding to all things cyber. Instead, policyholders will likely still have to rely on traditional products to bridge several coverage gaps. Even then, there are still areas of cyber risk that will be left uncovered. Nevertheless, these stand-alone cyber liability policies are a step in the right direction. Additionally, the current "soft" market for these policies invites the opportunity for policyholders to closely examine their cyber exposures, and bargain with insurers in a meaningful way for expanded coverage that is needed, and to opt-out of paying extra premium for coverage that is not necessary given the company's risk profile. As stand-alone cyber policies are structured to place the burden on policyholders to demonstrate coverage, one way in which policyholders can maximize their policy is by identifying coverage limitations, and moving them to the "exclusions" section of the policy to place the burden of excluding coverage on the insurer. Likewise, insurers can utilize their underwriting and claims experience with prior policies and forms to conform the cyber policies in a manner that will not only accord with the policyholders' expectations, but will eliminate at least some of the risk inherent in policies that have not been tested in court.

1. See, e.g., *Zurich American Insurance v. Sony Corp. of America*, 651982/2011 (Sup. Ct., N.Y. Cty., 2011) (finding no coverage available under CGL policy for data breach); *Recall Total Info. Mgmt. v. Fed. Ins.*, 147 Conn. App. 450, 463-4 (Conn. App. 2014) (holding that suspected dissemination of personally identifiable information not covered under CGL policy).

2. See, e.g., *Palkon v. Holmes*, No. 14-cv-01234 (D.N.J. 2014), in which plaintiff, a shareholder of Wyndham Worldwide, sued the hospitality giant on similar theories of liability after learning of three separate data breaches allegedly resulting in the theft of over 600,000 customers' PII).

3. 8 Del. C. §145(b).

4. *Consol. Edison of N.Y. v. Allstate Ins.*, 98 N.Y.2d 208, (2002) (noting that, ["generally, it is for the insured to establish coverage and for the insurer to prove that an exclusion in the policy applies to defeat coverage"]; *Tarry Realty v. Utica First Ins.*, 2013 NY Slip Op 33603(U), at *10 (Sup. Ct., NY Cty. 2013) (holding that, in an insurance coverage action, the insured bears the initial burden of showing that the "insurance contract covers the loss for which the claim is made. The burden then shifts to the insurer to demonstrate that a policy exclusion defeats the insured's claim") (citations omitted).

5. *Bridge Metal Indus. v. Travelers Indem.*, 559 Fed. Appx. 15 at * 17 (2d Cir. 2014), citing *Fed Ins. v. IBM*, 18 N.Y.3d 642, 965 N.E.2d 934, 936, 942 N.Y.S.2d 432 (N.Y. 2012).

6. *Bridge Metal Indus.*, 559 Fed. Appx. 15 at * 17 (internal citations omitted).