CFO

CYBER INSURANCE POLICIES: ARE THEY WORTH THE MONEY?

Under a dedicated cyber insurance policy there's no "standard" liability coverage available.

BY LYNDA BENNETT

cfo.com

Cyber security concerns and massive data breaches are part of our daily news cycle. As a result, companies of every size and industry are carefully examining their cyber security preparedness, both as a matter of good business and because they are being forced to do so by regulators and their customer and client base. An integral part of that self-reflection process is (or at least should be) the availability of insurance coverage for the risks presented by security breaches.

Some companies have purchased "dedicated" cyber insurance policies that provide coverage for first-party and third-party risk exposures. Other companies are still in the evaluation phase and are appropriately wondering whether such policies are needed, and, if so, whether insurers are paying claims under them.

Lynda Bennett

Are We Covered for That?

At present, the only meaningful generality that can be made about the scope of coverage available under a dedicated cyber policy is that there is no "standard" coverage available. Several different insurers are offering cyber liability coverage and the nature of what is covered versus what is not varies significantly.

In addition, many of these policies include a series of coverage enhancements that can be added to the policy, sometimes at no additional premium. But the policyholder must be a savvy consumer who makes the right "ask" and has a good handle on the risks that it is seeking to insure.

For example, some insurers are willing to provide coverage for PCI-DSS assessments while other insurers are not. Moreover, many insurers willing to provide coverage for this type of claim will not provide "full limit" coverage for the risk exposure and instead will place a "sub-limit" for such claims. The insurer's willingness to provide this coverage, and the extent of limit available for it, will depend on the number of records handled, the strength of the insured's existing procedures to prevent security breaches, and the data breach claims history.

Are Claims Being Paid?

We are still in the very early stages of evaluating the claims history associated with cyber insurance policies. For the past several years, insurers have been grappling with how to underwrite the risks that will be insured, how to offer the "right" limits, and how to appropriately price the policies, both in terms of premiums and self-insured retentions.

So far, there is anecdotal evidence to support the proposition that some of the headline- grabbing data breaches involved recovery of at least some cyber

insurance. But we have not yet seen the emergence of hotly contested coverage litigation associated with new cyber insurance policies. Rather, most court battles addressing security and data breaches continue to focus on the availability of coverage under "traditional" insurance policies.

In some instances, we have seen insurers pay a claim because there was an extremely low sub-limit and the insurer recognized that the scope of the loss far exceeded any coverage fight worth having. In other instances, we have seen policyholders manage the size and scope of the risk to a level that stays within the (often very high) self-insured retention such that the insurer is not required to pay.

But earlier this year, there was an interesting lawsuit filed that suggests insurers may be prepared to pay their insureds' claims and then pursue recovery from responsible third parties. In that case, Travelers Casualty and Surety Co. of America paid a claim submitted by its policyholder for a security breach that resulted from a hacking event.

The policyholder, Alpine Bank, had hired a professional designer to design the company's website and maintain the host server. Hackers accessed the website and gained entry to customer information. As a result, the policyholder was required to incur significant breach-notification costs.

Travelers paid the claim and then sued the designer, alleging that the designer failed to place basic anti-malware software on the server and failed to maintain adequate encryption controls over the customer data. It is premature to predict the outcome of the lawsuit. Nevertheless, it does offer some hope that insurers intend to stand by the coverage provided under cyber policies and then take up the fight to pursue responsible third parties for breach events.

How Do We Maximize Recovery?

There are two critically important steps that companies must take to maximize the likelihood and amount of their insurance recovery under cyber policies.

First, companies must take great care to conduct detailed and comprehensive due diligence during the application process of buying the cyber policies. Many insurers are requiring prospective insureds to supply a warranty letter along with a formal insurance application before issuing the cyber policy. Policyholders are well served to provide more, not less, information from the appropriate constituencies in connection with these requirements. Robust disclosure will reduce an insurer's attempt to cry "foul" after a loss has occurred.

Second, companies must understand the importance of providing timely written notice after a loss, even if the loss may not exceed the retention. The new cyber policies are written on a "claims-made" basis such that a delay in providing notice of the claim may result in complete forfeiture of coverage. Moreover, insurers will not give credit to dollar amounts spent against the retention unless and until they are on notice of a claim.

Lynda Bennett is a partner at Lowenstein Sandler LLP and Chair of the firm's Insurance Coverage Practice. She represents corporate policyholders in insurance coverage disputes.

Lowenstein Sandler

Lynda A. Bennett
Partner
T: 973.597.6338 I F: 973.597.6339
lbennett@lowenstein.com