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

Does Your Cyberinsurance Policy Have You Covered?: Part 2


Bob Steinberg
Latham & Watkins LLP


Peter Rosen
Latham & Watkins LLP


Margrethe Kearney
Latham & Watkins LLP


Neil Rubin
Latham & Watkins LLP


Martha O'Connor
Latham & Watkins LLP

Law360, New York (May 08, 2014, 3:33 PM ET) -- Following on our recent overview of cyberinsurance issues, this article reviews specific consideration when shopping for cyberattack coverage. Companies at risk to financial losses from cyberattack should take a careful look at the available cyberinsurance products and consider whether these products can play a role in their plans for managing cyber-risks. There are, however, real differences in the needs of companies in different industries that should be addressed. This is where the advice of a knowledgeable broker and counsel is invaluable.

There are over 20 carriers who currently write cyberinsurance policies.[1] Most of these carriers offer multiple coverages, and coverage must be crafted to each individual client. Some carriers have minimum revenue requirements, but as the market gains maturity, these carriers are bringing in more small to midsized insureds. Some carriers limit their coverage to nontechnology companies or prohibit certain types of insureds, such as universities or payment processors. Other carriers don't have this type of stated restriction but specifically target specific industries, such as retail, health care, or financial institutions. Available capacity is generally within the $10 million to $25 million range, with some carriers offering excess coverage with capacity of around $10 million.

The biggest difference in coverage between carriers is in breach remediation coverage, and with many carriers the extent of that coverage is negotiable. Most carriers do not require the insured to utilize designated service providers, but almost all provide discounted rates through their own providers. Of those carriers who have a time limit for remediation coverage, the most common time period is one year after the breach. Almost all of the

available policies cover losses caused by a failure to secure data, loss caused by an employee, acts of third parties and loss resulting from theft or loss of property. Carriers also offer policy extensions, such as for media liability.

Purchasing Cyberinsurance

As with any insurance procurement process, purchasing cyberinsurance is fraught with important decision points and requires careful consideration and negotiation of key policy provisions.

The first step in this process is always analysis of the specific coverage requirements for the policyholder. For example, is the policyholder a data vendor or a data owner?

A data vendor is the custodian of third-party information and is exposed to risk that third-party information will be accessed and disseminated, triggering obligations under privacy and other regulations and potentially resulting in third-party claims related to the improper dissemination. A data vendor may have contracts in place with third parties that address confidential information and the contractual liability exclusion discussed above may come into play.

A data owner, on the other hand, does not control third-party data but is exposed to risk that its own confidential information will be improperly accessed and disseminated. Other key considerations are whether the company has overseas operations, whether the company has call centers, the extent of the company's Internet operations and the company's reliance on cloud computing.

Once coverage requirements are established, the insured can evaluate the various form offerings presented by carriers and identify the desired coverage options. Once options are chosen, the underwriters will be informed about the scope of coverage and will begin the review process.

In the past, companies were sometimes subject to audits of their network systems to evaluate risk levels. Now it is more common for smaller companies to submit an application containing information relevant to a cyber-risk analysis. Larger companies participate in a call or in-person briefing, with presentations by key individuals in the company who are responsible for cybersecurity. The underwriters are able to ask questions and obtain additional information during these briefings.

While underwriters will focus on security technology implemented by the company, there is no specific technology preferred by underwriters in this process. Rather, underwriters will evaluate technology in combination with the policies and procedures in place for protecting confidential information and the people responsible for implementing those policies and managing the technology.

After the underwriters have evaluated the application, negotiations take place regarding key policy provisions and definitions. When seeking coverage, it is important to pull from a reasonably wide pool of carriers, because some carriers refuse to negotiate on certain provisions. In the process of obtaining coverage, it may become apparent that one or more coverages or exclusions could disproportionately impact the value of the policy for a particular company. If that is the case, it is important to have several carriers with whom to negotiate on these items.

Cyberinsurance Premiums

In many insurance markets, ballpark estimates of the cost of a given level of coverage can be provided to prospective policyholders. This is not so in the cyberinsurance market.

For some time, the lack of standardized pricing was thought to be due to the newness of the market and the lack of available data points for creating an "average price." However, the market is now more developed and there are many relevant data points. The more likely reason for a lack of standardized pricing is the specificity of each policy to the policyholder's individual situation and the lack of uniformity in the risks assumed by carriers.

At the outset, and as discussed more fully above, there are important differences between the base policies offered by carriers that impact pricing. Those differences are compounded by the reality that — if done correctly — the policies written in this space are very specific to the needs of individual companies. However, there are some key factors that do drive pricing of cyberinsurance policies.

The following considerations may carry different weight depending on the policy being written and the underwriter conducting the analysis.

- The insured's industry: Some industries have more significant exposure to personal health information or personally identifiable information. For example, companies in the health care industry are likely to have PHI. In the retail industry, companies might be further subcategorized based on characteristics like the number of credit card transactions processed yearly.
- Geographic spread of operations: Companies with a global footprint face different risks in different jurisdictions. The U.S. is a fairly litigious environment with significant privacy laws and regulations, which create significant legal exposure. Other jurisdictions may not have robust regulation or enforcement, reducing the risk of exposure from a breach.
- Limits sought by insured: The aggregate limit of coverage will certainly impact price, but limits in other key areas such as notification costs will also affect premiums. For example, many policies limit coverage for notifications to a set number of persons.
- Deductible/retention: A higher deductible or retention will generally operate to reduce premiums.
- Security and privacy controls: Companies that can demonstrate high-quality controls will generally see lower premiums. It is important to note that quality is not based solely on the technology used by a company to protect data. Rather, it is the combination of people, processes and technology that a company uses to safeguard PHI and PII. While some carriers continue to inflict lengthy applications on applicants, it is much more common to ask the company to participate in a briefing at which individuals with responsibility for management and security of PHI and/or PII provide information and respond to questions.
- Claims and loss experience: A company's history of loss will inform decisions on the likelihood of future losses.
- Data breach team choice: If the insured wants to utilize its own data breach team, rather than using the carrier's team, the premium will likely increase. Policies requiring the insured to use the carrier's data

breach team reflect the savings a carrier is able to realize as a result of providing high-volume business to chosen experts. Some carriers will not write a policy that permits the insured to choose its own data breach team.

This nonexhaustive list of factors illustrates why the pricing spectrum is so broad and unpredictable. Even two similar companies in the retail industry could face significantly different pricing because of loss history and security and privacy controls. Rather than asking whether a premium is standard for the market, prospective policyholders may be best served by focusing on the premium cost in light their own particular risk of loss.

—By Bob Steinberg, Peter K. Rosen, Margrethe K. Kearney, Neil A. Rubin and Martha L. O'Connor, Latham & Watkins LLP

Bob Steinberg and Peter Rosen are partners and Neil Rubin is an associate in Latham & Watkins' Los Angeles office.

Martha O'Connor and Margrethe Kearney are associates in Latham & Watkins' Chicago office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., The Betterley Report, Cyber/Privacy Insurance Market Survey, June 2013.