CORPORATE COUNSEL
An ALM Website
corpcounsel.com | October 6, 2016

What You Need to Know Now (and Ask Your Broker) About Cyber Insurance

From the Experts

Daniel Garrie

It is undeniably the age of the cyberattack. One need look no further than the headlines of the nearest newspaper to see that there has been an explosion in the frequency and gravity of cyberattacks. Companies face threats from every direction, ranging from nation state actors, cyber criminals, unsecure vendors and even malicious insiders. With a landscape so full of risk, companies increasingly are turning to cyber insurance in order to manage and mitigate their cyber risk.

One reason major companies have made this move is increased communication between the IT and risk management departments and their boards of directors. In part due to the above-mentioned headlines, these departments are able to communicate the fact that a premium payment is but a drop in the bucket compared to the costs associated with a cyber event.

That said, cyber insurance policies are highly specialized, and differ immensely from insurer to insurer. Purchasers must therefore become educated in the many nuances of cyber insurance to ensure that they are purchasing the right policy. With such a fragmented and inconsistent market, how can purchasers possibly make good governance decisions and properly limit their exposure?

©iStock/kathykonkle

There has been minimal litigation, and no established standard lexical set for dealing with cyber insurance policies. The current leading case is *P.F. Chang's China Bistro v. Federal Insurance*, where a court found that an insurer did not have to pay vendor-related costs associated with a data breach even though the policy covered "direct loss, legal liability and consequential loss resulting from cybersecurity breaches." The lack of clearly defined guidance in the industry has led some purchasers to put themselves in the hands of their brokers, reasoning that brokers have a fiduciary duty to their clients to identify and source appropriate insurance. While this may be a tempting option, cyber issues are truly complex. Not all brokers can

deal with the many nuances, and even those that can may ultimately be proven incorrect as cyber insurance issues begin to make their way to the courts. This means that in order to be in the best possible situation, companies must not rely on others, but educate themselves on the intricacies of cyber insurance.

Before discussing the specifics, it is important to understand the variety of services an insurer may provide the purchaser of those services. When considering an insurer's services, a purchaser must first determine whether the service adds value. For example, services such as training, providing procedures and protocols, breach response and crisis management all potentially provide immense value to a company.

One of the critical factors to consider, so you can fully benefit from those services, are the qualifications of the vendors that provide those services. For example, not all breach response firms are identical. One firm can hire college students, put them through a six-week boot camp, and call them analysts, while another competitively selects industry veterans to do the same work. Even though one firm may cost more than the other on paper, the quality of work and efficiency of the firm that employs the experienced industry veterans will likely neutralize or exceed any cost savings.

Accordingly, purchasers should look beyond compelling collateral, and spend the time doing the research, and possibly reaching out to third-party experts, to determine which services and servicers truly add value. Additionally, while there is a general baseline of cyber services offered by most insurers who offer cyber insurance products, different insurers may provide other unique services, which should also be carefully scrutinized.

Turning to the insurance products themselves, one important difference is between first- and third-party cyber insurance. First-party cyber insurance is when the insured (the first party) is paid by his or her insurer (the second party) in the event of a breach. This is the traditional setup for insurance, wherein a party seeks to mitigate its own risks. Third-party cyber insurance is when liability insurance purchased by an insured (the first party) from an insurer (the second party) provides protection against the claims of another (the third) party. The key distinction is that third-party insurance leaves the insured responsible for its own damages or losses, whether caused by itself or the third party.

Third-party insurance is critically important in the cyber context because many cyberattacks take circuitous routes through vendors, who must be able to protect themselves from the risk of the liability of the attacked company being placed on its shoulders. For example, in the now infamous Target Inc. data breach, the cyber criminals were able to gain access to Target's systems through its HVAC vendor. Target may be able to seek damages in the millions of dollars from that vendor, and, without proper third-party coverage, that vendor faces an existential threat. Plainly, due to the interconnectedness of companies, particularly in the cyber context, third-party cyber insurance is a must-have part of any policy.

The goal of this article is not to make you an expert on the nuances of cyber insurance. Rather, it is to tee up key issues to consider, and key questions to ask your insurance broker about any policy that you are considering. Here are some questions that may be very useful in understanding the policy you are considering:

- What security controls can be put into place that will reduce the premium?
- Will there by a required security risk review?
- What policies or procedures can be put in place to reduce or limit risk?
- The cybersecurity industry is changing very fast; how can you ensure that my policy stays current?
- Do all portable media/computing devices need to be encrypted?
- What about unencrypted media in the care or control of your third-party processors?
- Are malicious acts by employees covered?

While not a comprehensive list of questions and considerations, they are good starting points to foster a meaningful dialogue with your broker or insurer. Since cyber insurance is still a developing product, those that seek to purchase it should be sure to take the necessary steps to make informed decisions that will result in proper coverage and real risk management.

The thoughts expressed in this article are solely those of the author.

***Daniel Garrie** is the executive managing partner at Law and Forensics. He is a forensic neutral, an arbitrator and technical special master with JAMS; editor in chief of the Journal of Law and Cyber Warfare (JLCW); and a partner at Zeichner Ellman & Krause.* *He would like to thank Yoav Griver, Michael Mann, Masha Simonova and Benjamin Dynkin as contributors.* *Contact: Daniel@lawandforensics.com.*