CYBER INSURANCE AND THE DEFENSE CONUNDRUM

by Craig R. Blackman, Esquire

Cyber risk and cyber insurance have been hot topics for several years now. Cyber risk is reported to be increasing exponentially year-to-year and is being evaluated by more organizations as the cyber threat profile increases.

One of the most substantial cyber risk corridors is related to the operations of that business's third-party vendors. The statistics regarding the consequences of a cyber breach event are telling. By the start of 2017, the average cost of responding to a breach was $665,000. The average cost per record involved was $17,000. Crisis service expenses averaged $357,000, while legal defense expenses averaged $130,000 and the average legal settlement was $815,000. See NetDiligence 2016 Cyber Claims Study. According to the senior claims director responsible for first-party cyber claims at one of the major U.S. market insurance carriers, incidence rates of cyber breach reports are increasing by 100 percent each year.

Cyber insurance is being offered by more and more insurers, and the scope and terms of that insurance varies, sometimes markedly, from carrier to carrier. The breadth of necessary or recommended cyber insurance protection varies from business to business and from industry to industry. Because of the variability of coverage provided by the many discordant policies now in or entering the cyber insurance marketplace, procuring the correct cyber coverage for your business can be complex and time-consuming as you evaluate the cyber risk arising from your own business's operations and third-party vendors.

There has been a lot of discussion about the various types of cyber risks that businesses face today and the various types of coverage available to address those risks. These risks can include costs related to forensic investigation to determine the nature and scope of the cyber loss, legal advice, business interruption, post-breach notification obligations, credit monitoring obligations, crisis management, reputational harm, cyber extortion, cyber theft, and data loss or destruction. And those are just the first-party loss exposures of the subject enterprise. Third-party liability risks include claims brought by customers or employees suffering a breach of privacy due to a cyber event; claims for statutory violations or common-law breach of contract or negligence claims arising out of a cyber event; and costs for responding to regulatory inquiries relating to the cyber event, including costs associated with investigations, fines and penalties.

Despite all that has been published and publicized, very little has been said about the practical application of that coverage to a loss event. And this is where the defense conundrum lies. While "conundrum" has many meanings, it is used here as meaning a puzzle or a problem.

In the cyber insurance defense conundrum there is one key factor that your broker probably hasn't pointed out to you and that your insurer doesn't typically put on your Declarations page. Cyber insurance policies often work differently than most other insurance coverages in your portfolio in that your defense costs likely erode your coverage limits despite that defense being controlled by your insurer.

Most internal risk managers (or those otherwise responsible for the purchase of insurance for their business or employers) are accustomed to two standard models of insurance coverage where defense costs are concerned. First, as is the norm in the Comprehensive General Liability (CGL) insurance context, the defense of claims that fall within the coverage (or potential coverage) of the subject insurance policy is controlled and provided by the insurer, usually by counsel selected by the insurer. When the insurer controls the defense under these policies, defense costs typically are paid by the insurer over and above the coverage limits of the policy. Second, as is the norm in the Directors and Officers (D&O) insurance context, the defense of claims that fall within the coverage (or potential coverage) of the subject insurance policy is generally controlled and provided by the insured, not the insurer. In those instances, where the insured controls its own defense, defense costs typically erode the policy's coverage limits.

However, cyber insurance policies tend to buck that norm. Most, although not all, of the most comprehensive cyber insurance policies on the market today assign the control of the defense of claims to the insurer while at the same time eroding the insured's policy limits.

Yes, you read that correctly: It is not uncommon in the cyber insurance market that the insurer controls the defense of claims under the policy, while the costs of that insurer-controlled defense erode the limits of coverage otherwise available to the insured. This raises the situation where an aggressive defense under the control of the insurer may leave little of the policy coverage limit left for any indemnity obligation if that defense fails or settlement ultimately is deemed appropriate.

With little experience regarding actual cyber event lawsuits and their financial outcomes, and recognizing that defense of even meritless claims can be time-consuming and costly, insurers using this approach have a finite risk: the policy limit. The finite risk allows insurers to price their coverage more competitively than might otherwise be possible in the absence of actual risk exposure experience.

That said, and despite the possibly logical genesis for this development, this still means that insureds who would usually expect that defense provided by their insurer will not erode their policy coverage limits should be on guard in this situation. Insureds need to understand whether the cyber policy they are selecting operates in this manner, and then they need to evaluate whether the coverage limits they initially selected should be increased to address this reality.

CONCLUSION

Many policy forms in the developing cyber insurance marketplace give the insurer control of the defense of potentially covered claims, while the costs of that defense erode the otherwise applicable policy limits available to the insured for coverage for any liability. This is a relatively unusual circumstance insofar as insurance policies with an insurer duty to defend are concerned. Insureds need to be aware of this anomaly to ensure they are purchasing appropriate limits of coverage for these risks, or are otherwise selecting a cyber coverage form in which they control their own defense or in which, although controlled by the insurer, the defense costs are in addition to, and do not erode, the otherwise available policy coverage limits.

Craig Blackman, a Partner in the Philadelphia office of Stradley Ronon, LLP, is a nationally recognized authority on the National Flood Insurance Program, and focuses his practice on a variety of insurance industry issues, including commercial and personal lines; environmental; cyber; directors & officers and errors & omissions; general liability; land title; fidelity and surety; and professional, employment and products liability. He has counseled clients on primary, umbrella, excess policies and reinsurance, as well as captive, self-insured and surplus lines programs; and proof of claim/coverage analyses in receivership. He also is a member of the firm's nonprofit & religious organizations practice group, representing nonprofit companies and related individuals regarding insurance needs of such entities and their boards, as well as the firm's Cyber/Privacy practice group.