

CYBER INSURANCE *Litigation*

Many insurance coverage disputes can be, should be, and are settled without the need for litigation and its attendant costs and distractions.

However, some disputes cannot be settled, and organizations are compelled to resort to courts or other tribunals in order to obtain the coverage they paid for, or, with increasing frequency, they are pulled into proceedings by insurers seeking to preemptively avoid coverage. As illustrated by CNA's recently filed coverage action against its insured in Columbia Casualty Company v. Cottage Health System,¹ in which CNA² seeks to avoid coverage for a data breach class action lawsuit and related regulatory investigation,³ cyber insurance coverage litigation is coming. And in the wake of a data breach or other privacy, cybersecurity, or data protection-related incident, organizations regrettably should anticipate that their cyber insurer may deny coverage for a resulting claim against the policy.

Before a claim arises, organizations are encouraged to proactively negotiate and place the best possible coverage in order to decrease the likelihood of a coverage denial and litigation. In contrast to many other types of commercial insurance policies, cyber insurance policies are extremely negotiable and the insurers' off-the-shelf forms typically can be significantly negotiated and improved for no increase in premium. A well-drafted policy will reduce the likelihood that an insurer will be able to successfully avoid or limit insurance coverage in the event of a claim.

Even where a solid insurance policy is in place, however, and there is a good claim for coverage under the policy language and applicable law, insurers can and do deny coverage. In these and other instances, litigation presents the only method of obtaining or maximizing coverage for a claim.

When facing coverage litigation, organizations are advised to consider the following five strategies for success:

1 TELL A CONCISE, COMPELLING STORY

In complex insurance coverage litigation, there are many moving parts and the issues are typically nuanced and complex. It is critical, however, that these nuanced, complex issues come across to a judge, jury, or arbitrator as relatively simple and straightforward. Getting overly caught up in the weeds of policy interpretive and legal issues, particularly at the outset, risks losing the organization's critical audience and obfuscating a winningly concise, compelling story that is easy to understand, follow, and sympathize with. Boiled down to its essence, the story may be—and in this context often is—something as simple as:

"They promised to protect us from a cyber breach if we paid the insurance premium. We paid the premium. They broke their promise."

2 PLACE THE STORY IN THE RIGHT CONTEXT

It is critical to place the story in the proper context because, unfortunately, many insurers in this space, whether by negligent deficit or deliberate design, are selling products that do not reflect the reality of e-commerce and its risks. Many off-the-shelf cyber insurance policies, for example, limit the scope of coverage to only the insured's own acts and omissions, or only to incidents that impact the insured's network.

Others contain broadly worded, open-ended exclusions like the one at issue in the Columbia Casualty case, which insurers may argue, as CNA argues, vaporize the coverage ostensibly provided under the policy. These types of exclusions invite litigation and, if enforced literally, can be acutely problematic and flat-out impracticable in this context.

There are myriad other traps in cyber insurance policies—even more in those that are not carefully negotiated—that may allow insurers to avoid coverage if the language were applied literally.

If the context is carefully framed and explained, however, judges, juries, and arbitrators should be inhospitable to the various "gotcha" traps in these policies. Taking the Columbia Casualty case as an example, the insurer, CNA, relies principally upon an exclusion, entitled "Failure to Follow Minimum Required Practices," which, as quoted by CNA in its complaint, purports to void coverage if the insured fails to "continuously implement" certain aspects of computer security. In this context, however, comprised of the extremely complex areas of cybersecurity and data protection, any insured can reasonably be expected to make mistakes in implementing security and this reality is, in fact, a principal reason for purchasing cyber liability coverage in the first place.

Indeed, CNA represents in its marketing materials that the policy at issue in Columbia Casualty offers "exceptional first- and third-party cyber liability coverage to address a broad range of exposures," including "security breaches" and "mistakes":

Cyber Liability and CNA NetProtect Products

CNA NetProtect fills the gaps by offering exceptional first- and third-party cyber liability coverage to address a broad range of exposures. CNA NetProtect covers insureds for exposures that include security breaches, mistakes and unauthorized employee acts, virus attacks, hacking, identity theft or private information loss, and infringing or disparaging content. CNA NetProtect coverage is worldwide, claims-made with limits up to \$10 million.

It is important to use the discovery phase to fully flesh out the context of the insurance and the entire insurance transaction in addition to the meaning, intent, and interpretation of the policy terms and conditions, claims handling, and other matters of importance depending on the particular circumstances of the coverage action.

3 SECURE THE BEST POTENTIAL VENUE AND CHOICE OF LAW

One of the first and most critical decisions that an organization contemplating insurance coverage litigation must make is the appropriate forum for the litigation. This decision, which may be affected by whether the policy contains a forum selection clause, can be critical to potential success, among other reasons, because the choice of forum may have a significant impact on the related choice-of-law issue, which in some cases is outcome-determinative. Insurance contracts are interpreted according to state law, and the various state courts diverge widely on issues surrounding insurance coverage. Until the governing law applicable to an insurance contract is established, the policy can be, in a figurative and yet a very real sense, a blank piece of paper. The different interpretations given the same language from one state to the next can mean the difference between a coverage victory and a loss. It is therefore critical to undertake a careful choice of law analysis before initiating coverage litigation, selecting a venue, or, where the insurer files first, taking a choice of law position or deciding whether to challenge the insurer's selected forum.

4 CONSIDER BRINGING IN OTHER CARRIERS

Often when there is a cybersecurity, privacy, or data protection-related issue, more than one insurance policy may be triggered. For example, a data breach like the Target breach may implicate an organization's cyber insurance, commercial general liability (CGL) insurance, and Directors' and Officers' Liability insurance. To the extent that insurers on different lines of coverage have denied coverage, it may be beneficial for the organization to have those insurance carriers pointing the finger at each other throughout the insurance coverage proceedings. Again, considering the context, a judge, arbitrator, or jury may find it offensive if an organization's CGL insurer is arguing, on the one hand, that a data breach is not covered because of a new exclusion in the CGL policy and the organization's cyber insurer also is arguing that the breach is not covered under the cyber policy that was purchased to fill the "gap" in coverage created by the CGL policy exclusion. Relatedly, it is important to carefully consider the best strategy for pursuing coverage in a manner that will most effectively and efficiently maximize the potentially available coverage across the insured's entire insurance portfolio and each triggered policy.

5 RETAIN COUNSEL WITH CYBER INSURANCE EXPERTISE

Cyber insurance is unlike any other line of coverage. There is no standardization. Each of the hundreds of products in the marketplace has its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer—and even between policies underwritten by the same insurer. Obtaining coverage litigation counsel with substantial cyber insurance expertise will assist an organization on a number of fronts. Importantly, it will give the organization unique access to compelling arguments based upon the context, history, evolution, and intent of this line of insurance product. Likewise, during the discovery phase, coverage counsel with unique knowledge and experience is positioned to ask for and obtain the particular information and evidence that can make or break the case—and will be able to do so in a relatively efficient, streamlined manner. In addition to creating solid ammunition for trial, effective discovery often leads to successful summary judgment rulings, which, at a minimum, streamline the case in a cost-effective manner and limit the issues that ultimately go to a jury.

Likewise, counsel familiar with all of the many different insurer-drafted forms as they have evolved over time will give the organization key access to arguments based upon both obvious and subtle differences between and among the many different policy wordings, including the particular language in the organization's policy. Often in coverage disputes, the multimillion dollar result comes down to a few words, the sequence of a few words, or even the position of a comma or other punctuation.

Following these strategies and refusing to take "no" for an answer will increase the odds of securing valuable coverage.



¹ No. 2:15-cv-03432 (C.D. Cal.) (filed May 7, 2015).

² The named plaintiff is CNA's non-admitted insurer, Columbia Casualty Company.

³ CNA's preemptory suit was dismissed without prejudice by order dated July 17, 2015 because CNA failed to exhaust alternative dispute resolution procedure in its policy.

AUTHOR

Roberta Anderson
Director
412.297.4794
randerson@cohenlaw.com