Cyber Insurance: One Key Step to Maximizing Recovery under Your Insurance Tower

By David E. Wood and John L. Corbett, Anderson Kill

As data breaches and other forms of electronic theft and sabotage multiply and take ever new forms, cyber insurance is fast becoming a must-buy for businesses in a wide variety of industries. Insurance companies have rushed to fill the need with a wide variety of specialty policies and endorsements. On the plus side, savvy insurance shoppers can often find good cyber coverage at reasonable prices. At the same time, the wide variety of products and skimpiness of claims history on this front make it challenging to know what you are buying and to match cyber insurance offerings to your particular risks.

The lack of uniformity in cyber insurance products makes purchase of excess insurance particularly challenging on this front. The stakes are high, as the magnitude of losses and liabilities stemming from cyber breaches keep expanding. Many companies are purchasing cyber insurance programs well into the tens of millions of dollars, if not in excess of $100 million.

These programs are generally comprised of multiple layers of insurance policies. The primary layer kicks in after the insured absorbs a specified amount of loss, known as a self-insured retention. Above the primary layer are "follow-form" excess policies, which largely mirror the scope of coverage afforded by the primary policy. Each excess policy is tapped once the underlying layer is exhausted by payment of defense costs, settlements, judgments or first-party loss. Or at least that is how most policyholders ***believe*** it works. Recent litigation history, however, has made the expected progress through the coverage tower problematic – and the problems are likeliest to emerge in newer lines of coverage like cyber.

Every excess policy contains a provision stating how coverage is triggered. Often, this consists of little more than the requirement that the underlying limits must be exhausted. Many excess policies, however, go further into specifying ***how*** the underlying limits must be exhausted for coverage to attach. For example, some policies provide that coverage is triggered only when the underlying limits are paid in actual currency, or that the payment must be made by the insurer.

For many years following *Zeig v. Massachusetts Bonding & Insurance Co.*, 23 F.2d 665, a 1928 decision by the Second Circuit Court of Appeals, courts took the view that, regardless of how these trigger provisions were worded, all that was required was that ***someone*** pay the underlying limits. According to *Zeig*, the excess insurer had "no rational interest" in whether the underlying insurer itself paid its full limits. Indeed, there was a practical reason for this approach: "To require an absolute collection of the primary insurance to its full limit would in many, if not most, cases involve delay, promote litigation, and prevent an adjustment of disputes which is both convenient and commendable." *Id.* at 666.

In 2008, the California Court of Appeal issued an opinion that rejected this public-policy-based approach. In *Qualcomm, Inc. v. Certain Underwriters at Lloyd's, London*, 161 Cal. App. 4th 184, the court held that, where an excess policy specifies that coverage is triggered by exhaustion of underlying insurance by payment ***by the insurance company***, public policy considerations cannot be placed above the plain meaning of the terms of coverage. Now, the proverbial Devil is truly in the details.

The *Qualcomm* decision rocked the insurance industry. Policyholders that were previously incentivized to settle with their primary insurers to resolve coverage disputes had little choice but to fight coverage battles to an all-or-nothing finish in an effort to keep any hope alive of tapping their excess insurance. Although the *Qualcomm* decision was not binding outside of California, insurance companies and policyholders alike were aware that other courts could follow suit. This prompted a number of insurance companies to revise their excess policy forms to include the requirement that underlying insurance be exhausted by payment by the underlying insurer.

Qualcomm presents a particularly daunting challenge for businesses, especially media content and internet service providers seeking to transfer sizeable risk exposure through cyber insurance policies. While other types of insurance either utilize well-litigated standard forms (Commercial General Liability insurance) or apply relatively common coverage structures (Directors & Officers Liability insurance), cyber insurance policies differ greatly in scope, structure and verbiage from one insurance company to the next. Moreover, while CGL and D&O policies are concerned with liability in relatively well developed areas of the law (tort, corporate and securities law), cyber insurance policies provide coverage in a rapidly changing intersection between law and technology. Sometimes, cyber policies continue to use language which has become outmoded or evolved in application in the years since it was drafted. At the other extreme, insurance companies attempting to corner new technologies and liability portfolios may utilize terms that are untested in courts of law or have not arrived at a commonly-understood meaning in connection with underlying technology.

Because of the "Wild West" nature of cyber insurance, coverage disputes unfortunately are not uncommon. Policyholders and insurance companies may find themselves at odds as to whether a policy was intended to cover a particular technology, the type of information or media at issue, or the means by which the information or media is transmitted. In some instances, insurance companies have disputed whether, under the terms of cyber insurance policies, separate claims involving similar technologies are related for purposes of coverage – thus drawing into question which policy even applies to a given claim.

In this environment, policyholders and insurance companies may be tempted to split the difference in a settlement, rather than spend years fighting a complex coverage dispute through the courts. However, where the policyholder is exposed to company-ending liability well into its excess insurance layers, and those excess policies contain *Qualcomm*-type language, that policyholder has little choice but to keep fighting with its primary (or lower-layer excess) insurance companies to ensure that the excess insurance remains within reach.

For this reason, policyholders purchasing multiple layers of cyber insurance policies may be well served by ensuring that their risk managers and brokers obtain endorsements to their excess policies that clearly exclude any *Qualcomm* language. This could be as simple as an endorsement in each excess policy providing that excess coverage attaches once the underlying insurance is exhausted by payment by the underlying insurer ***and/or the insured or anyone on behalf of the insured***. While this may result in the policyholder paying a higher premium, limiting the number of insurance companies that are willing to do business, the end result is that the policyholder has some leeway to settle with its lower-layer insurance companies for less than policy limits, pay the remainder of those limits with its own funds, then tap into its excess insurers' funds to resolve large-scale litigation. This may be a small price to pay to ensure that the policyholder will be around to continue to reap the benefits of the internet revolution.