The First Cyber Insurance Disputes are Hitting the Courts

6.1.2015

These days businesses large and small are grappling with the thorny issue of whether they need to buy insurance against data breaches and other kinds of "cyber liability," and, if so, what type of coverage to buy—and with what coverage limits. That task will be further complicated by inevitable judicial decisions interpreting new and unfamiliar language in cyber policies. The first round of those cases are beginning to land in court, giving insurance lawyers an inkling of the type of coverage disputes likely to emerge from this relatively new type of coverage.

Insurance lawyers have long been familiar with the pattern: a new kind of liability appears on the scene, insurers and their insureds dispute whether that liability is covered under standard general liability policies, the insurance industry develops a new kind policy to fill the perceived coverage gap, and—invariably it seems—new disputes between policyholders and their insurers crop up over the meaning of the new policy language. That can be dispiriting for policyholders, who occasionally find out the hard way that the new (often costly) policy they bought just last year doesn't provide the scope of coverage they thought it did.

That's what appears to be happening with cyber insurance. In one of the first cases to interpret a new cyber insurance policy, *Columbia Casualty Company v. Cottage Health System*, CNA is claiming that it does not owe coverage to its insured for a $4.1 million settlement entered into by the insured, Cottage Health Service, a California-based hospital system. The settlement ended a class action suit against Cottage Health by plaintiffs claiming that their personal information was compromised by a 2013 data breach involving over 32,000 confidential medical records. CNA is arguing that coverage is precluded by an exclusion in its cyber policy for the insured's "failure to follow minimum required practices." CNA's complaint emphasizes that the insured's alleged failure to "continuously implement the procedures and risk controls identified in its application" is

Related Services

Cybersecurity and Privacy Specialty Team

evidence of that failure. Filed in early May 2015, the case has not yet resulted in a judicial decision.

Cottage Health underscores the need for policyholders to carefully negotiate the wording of the language in cyber policies. A wide variety of such policies have recently hit the market, and many (but not all) contain highly subjective and open-ended exclusions, such as the CNA exclusion for "failure to follow minimum required practices." Such highly subjective language creates loopholes that can be invoked in any number of factual settings. They should be avoided at all costs. These days, what constitutes "minimim required practices" when it comes to cyber security is anyone's guess. Insureds should not leave that interpretation up to their insurers, who can be tempted to raise it to avoid coverage for major data-breach losses.

We have reviewed about dozen different cyber policies on the market today, and many of them contain highly subjective phrases like the one at issue in Cottage Health. Policyholders should keep in mind that for the most part insurers are anxious to establish market share for this relatively new type of coverage, and they can often be persuaded to eliminate highly open-ended language, which not only can appear in exclusions, but also can be "hidden" in policy definitions, conditions and limitations.

For more information on coverage for data breaches and cyber liability, contact Thomas Bick, the chair of Butzel Long's Insurance Coverage Specialty Team (bick@butzel.com), or any other member of the Insurance Team.