KILPATRICK TOWNSEND

Insights: Alerts

Cyber Risk Insurance Battles – The Need for Caution Begins Before the Policy is Purchased

June 17, 2015

Cyber risk events – hacking and other forms of data privacy breach – unquestionably have hit the big time. Multi-million dollar losses seem to be in the news every other day. When a company is hacked and private information is stolen, "secure" networks are reduced to shambles, business reputations are tarnished, and companies suffer loss.

Recognizing the full dimensions of these risks, companies are flocking to buy insurance. Insurance products on the market cover a wide range of loss including liability for security breaches, costs for defending against claims of stolen private information, network security repair costs, and other loss. More than 60% of businesses recently surveyed by the trade report *Business Insurance* acknowledged that they purchased specific cyber coverage, and many of those companies are buying tens of millions of dollars in policy limits. The purchasers broadly range across a wide swath of leading U.S. industry groups, including retail, health care, education, hospitality, and financial.

History teaches that when insurance coverage is sought for new types of liabilities (e.g., asbestos, environmental) or where new policies or language are placed in the market to respond to specific losses (e.g., environmental coverage, director and officer coverage), lawsuits are necessary to bring clarity to what is covered. We are quickly approaching that time with respect to cyber coverage, and the battles are beginning to rage. *What is clear from these emerging cases is that policyholders need to be attentive to and cautious about their security programs and insurance issues even before the cyber policies are purchased.*

A recently filed lawsuit in California highlights what will be a major battlefield when significant cyber claims are submitted for coverage. In that case, Columbia Casualty Company ("CNA") sued its policyholder, Cottage Health System ("Cottage") claiming there was no coverage for the $4.1 million settlement paid by Cottage to approximately 51,000 plaintiffs whose private medical information was stolen when a hacker broke into Cottage's data system. CNA had sold a "NetProtect360" insurance policy to Cottage. Unfortunately for Cottage, CNA now alleges the policy does not really provide 360-degree coverage.

Specifically, CNA asserted that a "Failure to Follow Minimum Required Practices" exclusion precluded coverage on the alleged ground that Cottage did not follow its own description of its data security system in the insurance application. CNA also asserted that Cottage's failure to follow the data security protocols detailed in its application constituted a misrepresentation, and that all coverage was forfeited as a result of that alleged misrepresentation. A trial ultimately may be necessary to determine whether there is coverage.

What the CNA case highlights is that policyholders need to be diligent from the first day that they submit an application for cyber insurance to make sure they understand the requirements for coverage in the event of a loss. Such applications should be completed

and reviewed carefully not just by risk managers, but also by the CIO, Chief Privacy Officer, or other cognizant IT professionals. Negotiations may be necessary to put correct coverage language in place. Then, after the coverage is purchased, policyholders must take care in implementing their cyber security practices, and create a record sufficient to prove that they have complied with policy requirements. At the end of the day, cyber coverage premium dollars are well spent only if covered losses are paid by the insurer, and the CNA case teaches that scrutiny is needed long before a loss is incurred in order to maximize the opportunities for recovery.

Kilpatrick Townsend's attorneys have extensive interdisciplinary experience dealing with cyber/data technology, insurance coverage, and privacy law issues. We are happy to assist in your review of cyber coverage and cyber risk technology matters. Please contact us if you would like to talk about these issues.