Daily Journal

Tug of war emerges in cyber policy claims

By Melanie Brisbon

Juliane Backmann / Special to the Daily Journal
Susan P. White, partner at Manatt, Phelps & Phillips, says she expects more data breach insurers to start to take harder lines on their coverage to try to reduce their exposure after policies have been issued.

After paying more than $4 million to settle a data breach class action filed against one of its policyholders, insurer Columbia Casualty Co. is seeking to recoup those funds by suing the policyholder and claiming it did not follow the "minimum required practices" for its cybersecurity policy.

Citing the ever-increasing number of data breaches in recent years, legal experts say the case could be the first of many of its kind, and will likely influence both the cyberinsurance industry and the laws relating to it.

According to Columbia Casualty's complaint, policyholder Cottage Health System, which operates a network of hospitals in Southern California, did not provide accurate information in its insurance application and did not follow outlined security risk controls - miscues that ultimately led to the exposure of 32,500 medical records. *Columbia Casualty Co. v. Cottage Health System* CV15-03432 (C.D. Cal., filed May 7, 2015).

"I think in the next two to three years, there will be more cases that will start to delineate some of the issues that are coming up," said Susan P. White, partner at Manatt, Phelps & Phillips LLP who specializes in complex insurance coverage matters. "I think what you're going to see is more insurers starting to take harder lines on their coverage to try to reduce their exposure after the policy has been issued."

The health care industry, White said, brings more complex challenges for cyberinsurers. She said health care data breaches often have more substantial issues than breaches in other industries.

"Not only would they have your basic credit card information and maybe your home address, they are also going to have additional information like private medical information that could cause higher losses," White said. "Those are the kinds of things the insurers are going to be looking at when they decide to underwrite a policy."

Data breaches were more frequent in health care than in any other industry in the last couple years, according to Navigant Consulting's Information Security & Data Breach Report from last year.

And it comes at a high cost for the industry: The Ponemon Institute estimates that data breaches is costing the health care industry $6 billion per year, according to their Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data published this year. More than 90 percent of health care organizations that participated in the study had experienced a data breach, and 40 percent had more than five data breaches over the past two years. The average cost of a data breach is $2.1 million, according to the institute.

Mark C. Mao, co-chairman of the data privacy practice at Kaufman Dolowich & Voluck LLP, said it may be more difficult for health care entities to get cybercoverage and they often face higher premiums in the marketplace.

"Health care companies seek data privacy counsel more often because such organizations historically have had more privacy incidents arise. They often have older security systems, while being subject to one of the longest standing set of privacy rules," Mao said. "For health care, their priority is typically to make sure that you are well."

"IT can become a secondary concern to non-tech companies," he added.

Shawn Dougherty, a spokesman for the Insurance Standards Office, which offers standard cyberinsurance forms and underwriting guidelines which can be used at the insurers' discretion, said that because cyberinsurance is a relatively new field, it can present insurers with many challenges, one of which is pricing.

"A lot of insurance companies would love to be able to compare their book of business to the industry as a whole," Dougherty said. "But from an industry perspective, there isn't one massive database of aggregated data."

Legal industry insiders say that the litigation involving cyberinsurance policies with likely increase. In the Columbia Casualty case, the insurer alleges that the company did not have the proper procedures in place to protect a server containing patient information and for that reason, the exclusion applies according to court documents.

Mark Mermelstein, co-chairman of the cybersecurity and data privacy group at Orrick, Herrington & Sutcliffe LLP, said that many insurance companies have similar exclusions in their policies.

"A number of cyber policies require that the insured institute minimum required cybersecurity practices, and eliminate coverage for any failure of the insured to continuously implement such procedures," Mermelstein said.

Mermelstein added that the Columbia Casualty case could impact how companies view their own cybersecurity going forward.

"I think the impact it would have regardless of how it's decided is that you would want to take some steps on the front end to try to negotiate away clauses like that," Mermelstein said. "The second effect I think it will have is to really force companies to take a good hard look at their cybersecurity on the front end. "

Matthew T. Walsh, an attorney at Chicago-based Carroll McNulty & Kull LLC who is counsel of record for the plaintiffs in the Columbia Casualty case, could not be reached for comment for this story. Linda D. Kornfeld, an L.A.-based partner at Kasowitz, Benson, Torres & Friedman LLP who is representing the defendants declined to comment specifically on the case.

Last week, Cottage Health System filed a motion to dismiss the case.

melanie_brisbon@dailyjournal.com