Friday, July 18, 2014

General liability policies may exclude data breach coverage

By Melanie Brisbon

As the number of data breaches has steadily increased year on year, so have insurance claims related to remedying the exposure of personal and financial data in their aftermath. But starting this summer, businesses may begin to find that their general liability policies no longer cover cyberbreak-ins.

The Insurance Services Office, which sets guidelines for insurance terms and pricing across the country, has endorsed a list of standard exclusions that insurers have begun to roll out to policyholders. Among them are damages for access to or disclosure of any person's or organization's confidential information and for damages relating to companies' lost data and corruption of electronic files.

"The purpose is to force companies to buy cyberinsurance by restricting their coverage under their general liability policies," said Reynold Siemens, a partner at Pillsbury Winthrop Shaw Pittman LLP who advises companies in insurance negotiations.

Standalone policies could cost companies anywhere from $1,000 to six figures, depending on the coverage, according to Nick Economidis, an underwriter for Beazley Insurance Services. The payouts can be used for investigating the breach, notifying those affected, paying fines, managing public relations and footing any legal battles that ensue.

American International Group Inc., or AIG, even offers coverage from bodily harm resulting from a cybersecurity failure.

Policies "could also potentially include business interruption fallout that results in a company's systems being down," said William Um, insurance attorney at Hunton &Williams LLP.

So-called denial of service attacks, in which hackers prevent users from accessing their information while demanding that the company pay a ransom, have become more powerful in recent years. Startups like Feedly, Evernote and others have experienced service disruptions this year by groups seeking a few hundred to thousands of dollars. In most cases, the companies worked around the clock to defeat the attacks, but some have also paid off the hackers.

Siemens said companies need to assess the potential threats to the company before identifying which products might best match their needs. And then, "you need to negotiate them like any business contract," he said. "Make sure that the terms and conditions are fully understood and that the terms and conditions are not unduly one sided."

In certain cases, attorneys say, clients that have discovered breaches long after they happened.

"People who have had their accounts hacked into may not have unauthorized transactions until six to eight months after," said Mark Mao, partner at Kaufman Dolowich & Voluck LLP. "How are you going to prove that when your account is hacked, that is the result of a breach?"

Further, companies may find that insurers are unwilling to cover cyberbreaches even if general policies don't explicitly exclude cybercrimes.

"What happens in those situations often is that the breach will be discovered later on and the company gets notified of that sometimes through a lawsuit and the company will tender that claim to the insurance company," Siemens said. "The insurance company will often deny that, claiming the breach happened after you bought the insurance policy."

Though many general liability policies exclude this, it is possible to find retroactive insurance that covers breaches that took place years prior.

"Companies need to be more vigilant in understanding their risk profile," Um said. "It's important for companies to match the risk with the multitude of insurance options that are currently available in the marketplace."

melaniebrisbon@dailyjournal.com