Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data Breach Report Shows Cyberinsurance Not A Cure-All

By **Jeff Sistrunk**

Law360, Los Angeles (March 15, 2016, 8:57 PM ET) -- A recent report on how companies are managing cyber risks shows that cyberinsurance isn't a panacea for all the problems that can result from a data breach and indicates that policyholders should consider bringing in outside firms to help mitigate the fallout from a breach, according to experts.

Here, Law360 examines the key takeaways from the report for policyholders.

Cyber Policies Aren't One-Size-Fits-All

The report, which was compiled by insurance analytics company Advisen Ltd. and data breach response firm ID Experts based on survey responses from 203 risk-management professionals, concluded that cyberinsurance is largely designed to protect against "low-frequency but high-severity" cyberattacks affecting many thousands of electronic records.

However, the report also determined that the costs associated with the majority of data breaches that hit the responding risk managers' companies fell below the deductibles in the companies' cyber policies. For large corporations, data breach response costs under the applicable deductible may not be much of a concern, but for smaller companies, those costs may be more significant, experts say.

"Cyberinsurance is by no means intended to be a one-size-fits-all solution," said Greg Podolak, leader of Saxe Doernberger & Vita PC's cyber risk practice.

Companies must appreciate how far-reaching their cyber risk exposure may be so they can tailor their cyberinsurance coverage accordingly, according to experts.

In years past, full insurance coverage was available for so-called "event management" services such as forensic analysis and data breach notification to customers, but those services are now typically subject to deductibles and retentions. Still, it is possible to obtain a cyber policy that has a lower deductible or retention for event management costs, experts say.

"There are some policies that have a retention or deductible that can be significantly lower for the costs of forensic investigation, breach letters or crisis management than the deductible for putative class actions and dealing with regulatory investigations," said Barnes & Thornburg LLP partner Scott Godes.

The report also highlights the need for companies to negotiate favorable retroactive dates in their cyber

policies so they will be covered in the event they were hit by an undetected data breach before obtaining the policy, Anderson Kill PC shareholder Joshua Gold said.

"From an insurance coverage standpoint, the report alludes to the fact that some policyholders are breached before they even know it," Gold said. "For cyberinsurance buyers, this highlights the need to get a favorable retro date for the policy — one earlier than the policy inception date."

Coverage Gaps Are Common

Even if a data breach is large enough to trigger coverage under a cyberinsurance policy, companies could still find themselves on the hook for part of the bill, according to the report.

In many cases, some of a company's losses may fall under one of the common exclusions found in cyber policies, such as those for damage to infrastructure because of a cyberattack or lost business or profits stemming from harm to the company's reputation in the wake of a breach. To avoid being uncovered for certain losses tied to a cyberattack, companies must identify any potential gaps in cyber coverage and strive to fill them, according to attorneys.

With respect to property damage, traditional first-party property policies will usually provide little reprieve because of the proliferation of exclusions for cyber-related incidents in such policies, experts say. But that may not always be the case, according to K&L Gates LLP partner Roberta Anderson.

"Property policies often have broad data-related exclusions and anti-concurrent causation language," Anderson said. "There may be exceptions to the data exclusion, though. It's dangerous to assume something is not covered."

In addition, American International Group and some carriers in the London insurance markets have started offering specialized "difference in conditions" insurance that can override cyber exclusions in first-party property policies.

"That type of DIC policy basically sits over traditional property insurance and unwinds the data-related exclusions that may be in that policy," Anderson explained. "A company can get the benefit of the physical-event trigger if they buy that coverage."

There is also a fledgling market for insurance covering a policyholder's loss of business because of reputational harm caused by a data breach.

"That coverage is nascent. It is by and large not available from many carriers," Anderson said. "It is still very much a growing product."

IT Shouldn't Tackle a Breach Alone

According to the report, 60 percent of the responding companies said they have tasked their IT departments with handling the response to a data breach.

While IT departments have a role to play in response efforts, "a sole reliance on IT can expose organizations to financial loss as breaches often require privacy and regulatory compliance," the report says.

"The approach to dealing with these issues has to be multidisciplinary; it's not just an IT problem," Podolak said, adding that a company's risk management and business development professionals should also be involved in data breach response.

Depending on the size of a company, the role an internal team is expected to have in a data breach response "can vary wildly," Podolak added.

"Most companies don't expect in-house resources to provide everything that's needed to respond to a data breach, nor should they," he said.

The report recommended that companies enlist the services of third-party data breach response vendors to handle a slew of services in the aftermath of a cyberattack, including forensic analysis, breach notification and public relations. Most cyber insurers will point their policyholders to well-regarded third-party firms that can help mitigate the fallout from a data breach, experts say.

"Even for large companies, those outside vendors often provide a level of service that they cannot implement using their own resources," Gold said. "For a small or midsize company, that advice is likely even more valuable."

Anderson said that companies should utilize multiple vendors to address each prong of a data breach response.

"If a breach ends up being far greater in scope, and you have regulators after you and are facing class action litigation, it is important to have multiple third-party vendors, especially a forensics vendor and breach coach counsel," Anderson said. "That will help the company mitigate its overall exposure and harm to their brand and reputation."

--Editing by Christine Chun and Philip Shea.