

5 Tips For Scoring Data Breach Coverage

By **Bibeka Shrestha**

Law360, New York (April 02, 2013, 8:06 PM ET) -- Data breaches can bring along staggering response and litigation costs, making it all the more important to get insurers to foot the bill. Here, attorneys tell Law360 how policyholders can do just that.

Look for Coverage Everywhere

Although cyber policies, which are specifically designed to cover data breaches, are becoming more popular, many companies are still going without them. But that doesn't mean they're out of luck when it comes to getting insurance for data breach costs.

Policyholders can look to general liability policies, property policies, crime insurance and even directors and officers policies as potential sources of coverage for costs including repairing damage to computer systems and battling class actions brought by customers who had their personal data exposed.

Orrick Herrington & Sutcliffe LLP partner Richard DeNatale said businesses that already have cyber policies should keep in mind that defense costs often count toward the policy limits, whereas the same isn't true for most general liability policies.

The more policies you look to, the more likely it is that all your costs will be covered.

"It's very important to check all your policies and not automatically assume it can't be covered because I've already bought a dedicated cyber policy," said Joshua Gold, a shareholder at Anderson Kill & Olick PC.

Keep Your Insurers in the Know

Companies reeling from data breaches often quickly turn their attention to notifying impacted customers and responding to government investigations — tasks that understandably can be overwhelming. But they shouldn't neglect to notify their insurers promptly of the breach.

"It's really easy to overlook the insurance component in the very early stages," said Tyler Gerking, a partner at Farella Braun & Martel LLP. "But to overlook the insurance component can be a big mistake."

Insurers frequently argue against coverage when companies provide late or incomplete notice, Myers said. Policyholders can nip that in the bud by telling insurers about a breach right away.

"You should really try to develop a good working relationship with your insurer," DeNatale said. "Keep them informed."

Get Insurers to Sign off on Costs

In the chaos surrounding a data breach, companies might offer credit monitoring or credit insurance, as well as indemnification to corporate clients that might be targeted over the breach — all of which can come with hefty costs.

"A company might want to go ahead and offer something to consumers or offer something to its corporate customers, to either remedy their losses or otherwise deal with the event," Gerking said. "Doing that without the insurer's consent can complicate the claim."

Insurers providing data breach coverage often require written consent for all those expenses, as well as the cost of hiring forensic consultants to determine the source of the breach. That can be the single largest expense, provided the policyholder isn't hit with a class action, according to DeNatale.

Getting an insurer to sign off on those costs weakens the potential argument that the expenses were voluntary and therefore not covered.

Talk to the Experts

Policyholders grappling with data breaches are often doing it for the first time. They should turn to claims-handling experts who have gone through the drill before, to make sure insurers aren't cutting corners or taking unreasonable positions on coverage.

Input from claims handling experts and forensic consultants can be particularly useful if policyholders and insurers wind up in court over coverage for large data breach claims.

"We've used those kinds of experts, whether in a testifying role or at least in a consulting role," Gold said.

But to prevent relationships with insurers from going sour, policyholders should look to the carrier itself for advice on responding to data breaches. Since insurers deal with data breaches more often and have their own share of expertise, this will smooth out the claims-handling experience.

"The insurer really can be a resource to the insured, because the insurer has more information," Gerking said.

Know Your Jurisdiction

If a company and its insurer can't see eye to eye on coverage and head to court, policyholders should realize that the forum for these legal disputes will be pivotal.

"Different jurisdictions are really all over the map when it comes to construing the policy provisions and exclusions on general liability policies that come into play on a data breach," said Marty Myers, a partner at Jones Day.

Courts weighing data breach coverage under commercial general liability policies vary widely on what counts as an invasion of privacy and what counts as publication of information — important questions that crop up when a company says its CGL policy's personal and advertising injury sections are triggered.

If you're a national or global company, pay attention to precedents that have already been set on data breach coverage in the state where the breach occurred, the state where the company is headquartered and the state where policies are underwritten.

"You really have to check your [policy] language, you have to check the state law, and obviously you have to check your facts," Gold said.

--Editing by Kat Laskowski and Richard McVay.

All Content © 2003-2013, Portfolio Media, Inc.