Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Insurers Grow Tentative About Coverage For Cloud Users

By **Bibeka Shrestha**

*Law360, New York (November 13, 2012, 9:46 PM ET)* -- Insurers are starting to scrutinize coverage for companies using third-party data services, seeing cloud providers as especially vulnerable to hacking attacks, and with cyberpolicy language constantly evolving, attorneys say policyholders should pay closer attention to whether their cloud-related losses would be covered in the event of a breach.

Last year, hackers reportedly used Amazon.com's cloud service to launch a cyberattack that compromised the account data of more than 77 million Sony Playstation users. But that much-publicized data breach hasn't slowed a trend of companies turning to remote data storage and handing over more and more sensitive data to cloud providers.

On the other hand, insurers that have long been leery of covering cloud providers that house massive amounts of third-party data are beginning to look more critically at cybercoverage offered to companies using cloud computing, experts say.

While insurance carriers typically evaluate security protocols at the companies they cover before issuing cyberpolicies, they're now scoping out the cloud providers their potential customers are using, according to Roy Hadley Jr., Barnes & Thornburg LLP partner and co-leader of the firm's cloud computing and cybersecurity practice team.

"Now you're seeing insurance companies step back and saying, 'Let me really start thinking about this risk, Who are you using for your service provider, what are their policies and procedures, because that's what really matters,'" Hadley said.

Insurers are still trying to get a good handle on how best to cover the risks associated with their insured's cloud service providers, and some may opt to offer lower policy limits or charge higher premiums for this kind of coverage, according to Hadley. Carriers are also pushing back more on paying data breach claims, Hadley said.

Some say that data is actually more secure with cloud providers since their main business requires them to stay up-to-date on security threats, but others point out that aggregating so much data from so many companies in one place creates too attractive a target for hackers. Insurers have especially grappled with quantifying these risks, experts say.

"They haven't been able to get their hands around the aggregation issue," said Kevin Kalinich, global practice leader of the cybersecurity team at Aon Risk Solutions.

Sherilyn Pastor, the leader of McCarter & English LLP's insurance coverage group, advised companies shopping around for cyberpolicies to step back and take a careful look at their own risks and whether the language in each policy intends to cover those risks.

"There's a kind of panoply of coverages that you can get," Pastor said. "You really do have to understand what your risks are so that you're buying coverage appropriate to whatever may be unique to your business."

Cyberpolicies that are written well should cover the costs of notifying impacted parties about a breach, hiring attorneys, investigators and specialists, as well as liabilities to third parties, according to Scott Godes, a Dickstein Shapiro LLP attorney who co-leads the firm's cybersecurity insurance coverage initiative.

It'll be important for corporate risk managers, the heads of information technology and in-house counsel to put their heads together to calculate risks associated with using the cloud, legal obligations and questions of insurance coverage, Godes said.

Companies should especially look at the definition of "computer system" and "network" in policies, since those terms can often dictate whether there's coverage for cloud losses, Godes added.

Shipping data to a cloud firm can often mean crossing not only state lines, but also international boundaries. Insurers will sometimes specify that their policies only cover losses caused by computer systems located in a certain place, according to Joshua Gold, an Anderson Kill & Olick PC shareholder.

"You need to make sure that you've got insurance coverage that's going to not be subject to some sort of territorial limit," Gold said. "You've got to look at every insurance policy provision because the fine print can absolutely kill you."

To minimize risks, policyholders should also be cautious when selecting a cloud provider, and ask which company is actually providing cloud services, what their security procedures and privacy policies are, what their indemnities are, and where exactly they plan to store data, Hadley said.

They should moreover examine whether cloud providers have physically secure data warehouses and whether they do background checks on their employees.

"If their employees are crooks, you've let them into the castle with a key," Hadley said.

Documenting the due diligence that companies carry out in choosing a cloud provider could be helpful in fighting against any potential lawsuits or regulatory actions stemming from data breaches, and also in challenging insurers' arguments that companies did not take all necessary steps to safeguard their data.

Companies can also try pressing cloud providers to provide indemnification for cloud-related losses, but most cloud firms have been unwilling to include their users as additional insureds in their policies, according to Godes.

"The idea is to lower the costs for storing data," Godes said. "If the cloud provider would take on full liability, they would probably view that as increasing their costs and not providing an efficiency for people that use the cloud."

Still, some major companies been able to hammer out contracts with $100 million in indemnification, according to Kalinich.

"It depends completely on leverage," Kalinich said.

When it comes to covering themselves, cloud providers typically buy insurance policies with high self-insured retentions, similar to a deductible, because of insurers' reluctance to provide coverage and also because it reduces their cost of providing evidence of insurance to customers, according to Kalinich.

Capacity in the insurance market for cyber-risk has gone up dramatically over the last several years, but that doesn't mean that insurers are stepping up in all cases.

"A lot of companies that need insurance coverage the most are not always the ones that can afford the biggest limits or will even be offered the biggest limits," Gold said.

--Editing by John Quinn and Jeremy Barker.