

Cloud Service Providers Say Data Security 'Not My Job': Study

By: Fahmida Y. Rashid

Originally published on eWeek.com May 7th, 2011

Who is responsible for securing customer data in the cloud? The cloud vendors don't think data security is their responsibility, according to a Ponemon Institute study.

The biggest complaint in the wake of recent data breaches, whether it's Sony or Epsilon, has centered on the lack of security controls in place to protect customer data. A recent Ponemon Institute report found that cloud providers don't think that's their job.

A shocking 73 percent of U.S. service providers and 75 percent of their European counterparts said their cloud services did not substantially protect and secure their customers' confidential or sensitive information, according to the recent Security of Cloud Computing Providers report from the Ponemon Institute. Nearly 62 percent of U.S. providers and 63 percent of European providers were not confident that their cloud applications and resources were secure.

Approximately 69 percent of cloud providers in the survey didn't believe securing the data was their responsibility. Just 16 percent of cloud providers felt security should be a shared responsibility. Vendors told the Ponemon Institute researchers they didn't always evaluate their systems and applications prior to deploying them to the customer.

The findings surprised the researchers, according to Larry Ponemon, the institute's founder.

The Ponemon Institute did a similar study in 2010 on cloud users where 35 percent of cloud users thought securing their data on the cloud was their responsibility and 33 percent thought it was a shared responsibility.

"Neither the company that provides the services nor the company that uses cloud computing seem willing to assume responsibility for security in the cloud," the researchers concluded in the report.

A majority of the surveyed vendors don't even have dedicated security personnel to oversee the security of their applications, infrastructure or platform, the report found. On average, providers allocated 10 percent or less of their resources to address security.

The findings weren't entirely grim. Over 81 percent of cloud providers said they had access to "highly-qualified IT security personnel" and 80 percent had confidence in their ability to "prevent or curtail viruses and malware infection." Another 71 percent said they could "secure sensitive or confidential information in motion" and "achieve compliance with leading self-regulatory frameworks."

Vendors reported that customers were not considering security when evaluating providers. The vendors believed that improving security and complying with policies were low priorities for their customers, according to the report. Organizations are adopting cloud-based services to reduce costs, to simplify deployment and to improve customer service, the surveyed service providers said.

The vendors may not be too far off the mark, since cloud computing users in last year's report admitted they were not "vigilant in conducting audits or assessments of cloud computing providers before deployment," the report said.

Cloud providers should not be faulted for giving what customers want, like fast and cheap deployments and business uptime, said Matthew Gardiner, director of security at CA Technologies. However, there are many recent reports showing that customers have higher expectations about security in the cloud, Gardiner noted.

Cloud customers should be aware of their responsibility to assess security risks before placing data in the cloud. As organizations become more aware of the risks of not securing the data, they will demand their cloud vendors pay attention to security, according to Ponemon. However, it remains the organization's responsibility to thoroughly "vet providers and their applications and infrastructure for their ability to safeguard information," before deployment. More organizations and vendors should be sharing responsibility for security, Ponemon said.

The Ponemon Institute polled 103 cloud service providers from the United States and 24 in six European countries for the CA-commissioned study. About 55 percent of the respondents offered software-as-a-service, followed by 34 percent offering identity-as-a-service, and 11 percent with platform-as-a-service. Approximately 65 percent of the respondents offered public cloud services, 18 percent offered private clouds and 18 percent had hybrid clouds.

Private-cloud providers "appear to attach more importance and have a higher level of confidence in their organization's ability to meet security objectives than providers of public and hybrid cloud solutions," the researchers wrote.