MINTZ

Things to do in 2012: Questions to Ask of Cloud Vendors

December 19, 2011 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Adoption of cloud computing is certainly on the increase -- but 2011 has seen evidence of some of the risks associated with moving to the cloud. Notable among the year's data breaches was **the breach at e-mail marketer** Epsilon Data. To quickly refresh your memory, Epsilon was the victim of a hacking attack, and once the perpetrator was inside the database, the hacker had unfettered access to hundreds of thousands of email addresses maintained for hundreds of Epsilon clients -- the classic "multi-tenant" scenario. A single system, when broken into, gives the perpetrator potential access to a wealth of data.

The Epsilon episode raises additional concerns about how secure any data is within a cloud-computing infrastructure, especially as the technology becomes more mainstream.

Rather than accepting standard click-through terms and conditions (for example, **Amazon Web Services**, Google Cloud, **Rackspace Cloud**), customers should be asking tough questions of cloud vendors before putting mission critical or personal information into the cloud. Utilization of cloud services by businesses in regulated industries (healthcare, financial services) requires such inquiry.

Since this is the time of the year for "top ten lists," here is this author's **Top Ten List of Questions For Cloud Providers**

10. What are the security procedures in place to protect the data center and how are employees with access to data vetted?

9. How does the customer know if (when) there has been a breach?

8. How many live copies (instances) of customer data are maintained?

7. What is the provider's retention period and what is the recovery plan? What happens on termination - how easy it is to get data back to move to a new service provider?

6. What about third party applications that are used to deliver the service? How is that security controlled?

5. What encryption technologies are used by the vendor to authenticate access to the services and to the data?

4. What are the vendor's terms with respect to ownership of the data? How does the vendor delete the data when the customer is no longer a customer?

3. Where does the live data "reside"? Can the customer dictate the terms of geographical location/storage of data? If not in the US, what laws regulate government access to customer data?

2. How many locations does the vendor have and how are they connected?

1. What is their service level agreement (SLA) and how is the customer compensated if those SLAs are not met?

These are by no means the only questions that should be asked, nor are they necessarily in order of what would be the most important questions for businesses in certain industry sectors.

The US government has been working on developing a uniform means of assessing and authorizing cloud services -- and the program may be illuminative for companies trying to do the same. A memo issued this month by the Chief Information Officer for the U.S. Office of Management and Budget sets out the

requirement that all agencies use the Federal Risk and Authorization Management Program (FedRAMP) when purchasing cloud services. Agencies have until June 2012 to start using FedRAMP, which established a set of approved security controls that cloud services must meet, along with an assessment process for authorizing the use of these services within the federal government.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.