Cloud Computing Security: A Status Report

M. R. Pamidi, Ph. D.
Senior Editor
IT Newswire

Introduction

Cloud Computing (CC) is gaining momentum and mindshare from enterprises as a way of controlling IT costs. At the same time, there are many issues preventing many organizations from fully embracing CC. Security, as we have discussed before, appears to be the top issue among those evaluating CC, the concerns being whether others, including your competitors, can access your data and how safe is your data in the cloud. The recent China-Google incident has raised even more concerns about cloud security. This paper discusses various security concerns and what is being done by vendors and standards bodies to mitigate these. Note, this brief doesn't claim to be complete; we plan to publish a separate report evaluating various cloud security product vendors, including SWOT analyses, in the coming weeks.

Top Security Risks

Cloud Computing is fearfully insecure and may never be 100% secure. This is akin to your home: You may live in a gated community, have a lock on your front gate, padlock on your front door, guard dogs, AND an electronic security system installed in your home. Each layer of security makes your home *more* secure, not *fully* secure. However, this doesn't prevent you from living in your home. Similarly, many organizations will embrace CC, knowing the risks and rewards involved.

Following are some of the top security concerns, this list being by no means complete:

1. **Phishing:** No security system is impregnable. Many SaaS and PaaS claimed their systems are secure, yet salesforce.com had a phishing attack in 2007; Google Gmail was attacked in October 2009; and Microsoft Windows Live Hotmail was attacked in October 2009, just to mention a few.

2. **Data Privacy:** HIPAA, California SB1386, 201 CMR 17.00, and similar regulatory requirements protect individuals' privacy; yet, many organizations, especially in the U. S., don't seem to take these seriously and often pay heavy fines for data breaches. For instance, whereas the EU favours strict protection of privacy, laws such as the U. S. Patriot Act in the U. S. grant government and other agencies with virtually limitless powers to access information, including that belonging to companies—all in the name of national security. But, as Benjamin Franklin said, "Those who would give up Essential Liberty to purchase a little Temporary Safety deserve neither Liberty nor Safety."

3. **Data Location:** Many countries require that information used there must stay there. (Hello, Las Vegas!) Here, the CC model breaks down and the concept of VMware's vMotion makes little sense.

4. **User Access:** If enterprise data resides outside with a cloud vendor, how can you ensure only authorized users are accessing it?

5. **Data Separation/Segregation:** Some organizations worry that their data in cloud may reside next to their competitors'. This fear may be uncalled for: You and your competitors may do business with the same bank, but do you worry about your money 'sitting' next to theirs?

6. **Data Recovery:** If your cloud site crashes, does your vendor have provisions for data backup and replication, disaster recovery, and data integrity?

7. **Vendor Viability:** Do you feel safe with your current vendor? Do you have contingency plans if your CC vendor goes out of business?

What are the vendors doing?

Cisco, EMC, IBM, SAP, and several other leading technology companies announced in March 2009 that they had created an Open Cloud Manifesto calling for more consistent security and monitoring of cloud services. However, Amazon, Google, Microsoft, and Salesforce.com are highly conspicuous by their absence from the membership list of this organization. Cloud Security Alliance appears to be a competing organization whose membership includes Cisco, Dell, HP, and Microsoft. Notably absent are Amazon, Google, and IBM. Other standards include ISO/IEC 27001, addressing third-party audits governing security of information and network systems, and SAS70 for auditing.

For its part, Microsoft at the Professional Developers Conference announced in November 2009 Project Sydney that creates a virtual network that ties together pieces of an application or processes running in various places so they all look like one logical system. Sydney addresses security in virtualized, multi-tenant environments in which customers are typically sharing datacenter resources. In addition to embedding greater security into the public cloud, Microsoft is planning to help customers build private cloud networks within their own datacenters, using the same software Windows Azure is based on. This appears to be Microsoft's answer to customers seeking answer to the question, "Where can we get a private cloud?"

Best Practices

For Cloud Users

- Ask your vendor where your data is kept and be aware of the data protection laws in various jurisdictions where you operate.
- Establish your risk appetite and see if your vendor can fill your diet.
- Ask your vendor to provide you an independent third-party security audit.
- Thoroughly evaluate QoS and SLAs and examine penalty-reward systems.
- Ensure you review your vendor's security policies on a regular basis (semi-annually, annually) and that you are notified immediately of any security breaches.
- Examine your vendor's disaster recovery, data protection, and contingency policies.
- This *could* be confidential information, but find out which third parties your vendor deals with and if they have to access your data.
- Explore whether your provider will accommodate your own security policies, which might be more stringent than theirs.

For Cloud Vendors

- Establish and publish your credible security policies.
- Describe your disaster and contingency planning.
- Maintain regular security audits.
- Publicize your QoS and SLAs.
- Offer reasonable prices for your products and services, so customers can achieve realistic ROI.
- Define your portability and interoperability goals.
- Be active in standards bodies and industry alliances.
- Don't oversell Cloud Computing; know its benefits and limitations.

