CONFERENCE CALLS
UNLIMITED
MORE THAN A CONFERENCE CALL

CONFERENCE CALLS UNLIMITED
Presents
A White Paper on Cloud Computing
Part 3

Cloud Governance

In the two previous articles, this white paper series examined

-The history of Cloud Computing ("The Origins of Internet-Based Computing"), and

-The Cloud's major players ("Putting Cloud Computing into Action").

This third article considers risk analysis in the Cloud.

Risk Areas

The Cloud represents economies of scale in data processing. It also demands business decisions that professionals must evaluate carefully. Issues in any business decision include: availability, security, privacy, auditing, dependency, regulation, authorization, and communications. The IT industry calls this issue Cloud Governance. The same is true for business decisions when implementing Cloud Computing.

With reference to communications, companies must examine transmission between Clouds, within Clouds, and among Clouds and earth. And more.

Standards

Each Cloud company currently adheres to a unique set of standards, making communications between Cloud providers difficult. The IT community is in the beginning phases of reaching agreement among the hundreds of Cloud companies as to what those standards should be. Eventually Cloud providers will reach a consensus for open standards in Cloud Computing with ratification by the IEEE and the World Wide Web Consortium.

Currently, once a business commits to a vendor, the decision is locked in. Open, agreed upon standards will make changing Cloud vendors less difficult.

The Playing Field

The brawny players in Cloud Computing, such as Amazon, IBM and Google, want a large say in setting these standards. They

will take great care that communications standards do not level the playing field and thus remove their competitive advantage.

The computing world watches as these various market forces play out to bring order to the latest frontier: the Cloud.

Who Is In Charge?

Once committed to the Cloud, a user or client depends upon providers for the services offered. A user cannot migrate to apps unless the provider allows it. That gives the Cloud vendor the power to decide who lives and dies. In a level playing field, all customers would have access to all the apps they can afford.

Nevertheless, a company considering Cloud vendors should take this possibility into consideration:

"Any time someone puts a lock on something you own, against your wishes, and doesn't give you the key, it's not being done to your benefit."
- (Cory) Doctorow's Law

What If Your Data Is Subpoenaed?

Once a client moves intelligence or data to a Cloud server, the client relinquishes control of that information. This intelligence could include social security numbers, driver's license numbers, credit card numbers, authorization codes, private personnel files, plans for new business ventures, attendance records and minutes from confidential business meetings, photos, blue prints, floor plans, search terms, many things that are very private.

Imagine the government subpoenas your data from your Cloud provider. Does this subpoena go to your company since it is your data being collected? No. The subpoena goes to the Cloud provider. Is the provider currently obligated to inform you, the client that your data is under government scrutiny? No. The vendor could relinquish the information without informing the client.

If the Cloud provider does not inform its client that the government is

collecting data, this delays the client's legal recourse. How large a risk is that to the client and the company?

On the other hand, if the data resides in the client's data center, the government must approach the company directly. The company would receive the subpoena, and be aware that agents are collecting private business records and data, and could take appropriate legal action.

Before forming a strategic business partnership you must determine the integrity of the proposed partner. The same is true when establishing a relationship with a Cloud provider. Some Cloud companies may not have strict standards for privacy and may share a client company's user profiles for ad targeting with marketing companies. So caveat emptor applies just as much to business in the Cloud as it does on earth.

Read the Fine Print—Always!

As a rule, always check the "Privacy Policy" and the "Terms of Use" fine print at the bottom of the Cloud vendor's web page. A company who pledges to inform the customer of governmental scrutiny or hacking attempts will announce its commitment in the fine print.

The Electronic Frontiers Foundation warns that the Cloud is treacherous in matters of privacy. They advise that mission critical intelligence should be kept in the company's own data centers where it is in their strict control.

Security

In today's business environment data centers guard against security threats 24/7. Using the Cloud for processing and storage doesn't mean that a business can forget about hacking threats. Security is just as much a safety issue in the Cloud as it is in a company's own data center. When negotiating a contract with a Cloud vendor, consider these auditing issues:
How safe is your data from outside hacking? If your data is phished[1] or pharmed[2] will your Cloud vendor inform you?

Spare Capacity

Cloud companies conduct business. They minimize costs and maximize profits. For efficiency, Cloud vendors want minimum hardware investment to meet client demand. If demand goes up abruptly or some problem diminishes supply, do Cloud vendors have enough reserve capacity to meet customer needs? If there is insufficient capacity in Cloud vendors, the entire Cloud system could slow to a crawl or crash completely. Currently Cloud vendors do not publish utilization rates. So clients cannot tell if their Cloud suppliers are approaching meltdown.

Power Outage

Different factors can bring down an entire Cloud network, including power outages, bugs within a program, interference between program modules, transportation issues, distributed denial of service hacker attacks. It happened to Amazon's AWS for eight hours in 2008 and to Google Apps for six hours in 2009.

In Amazon's case, the company posted the cause of the disruption and prevention measures for that type of interference reoccurring. Google chose not to inform its customers what caused the downtime and what it was doing about it.

This is a telling point about customer support. When a business's 3rd party Cloud vendor goes lights out, can you get answers as to what went wrong and how long your services will be hampered?

Encryption

Cloud computing is scalable and very cheap for data storage and processing, making it very attractive to companies. But how do Cloud companies protect data? One way is encryption.

For email, Hushmail and Mutemail automatically encrypt and decrypt all messages. For data encryption, PGP and its open source equivalent,

TruCrypt, are available. With these services, data is unreadable by anyone without the proper password to decrypt. This is fine as long as storage is the only concern.

But what about word processing, spreadsheet and database manipulation on Cloud servers? Imagine an investment company uses a Cloud database. It uploads customer information in an encrypted format. But to process the data, it must be decrypted and manipulated. In its decrypted form, that data is vulnerable to government surveillance, marketing preference analysis, or industrial espionage. Once the processing is complete, results can be encrypted. But with electronic records and redundancy factors outside the control of the client company, there is no guarantee that the data remains private.

How Do You Know Who to Trust?

As with all business decisions, you must evaluate Cloud security. Some of the evaluation of Cloud-based service offerings can be scrutinized in ways similar to standard offerings. Established Cloud companies take care not to jeopardize their brand or divulge customer information to marketers. So checking a Cloud vendor with the Better Business Bureau and the Federal Trade Commission is a good idea.

Another solution is to use trusted authorities. Verisign and TRUSTe are two companies that require compliance on privacy issues by their member companies. The Cloud vendor that subscribes to Verisign or TRUSTe shows its commitment to privacy values.

If your company commits to a Cloud-based site, are you completely dependent upon the service provider for feedback about your data's security? Or is there something you can do to monitor your information?

McAfee SiteAdvisor tests spyware and adware 24/7 with parallel automated robots. Client companies can use this site to test their own Cloud-based website or application.
See http://www.siteadvisor.com/

Summary

Evaluating whether or not to move your data center into the Cloud demands more than a cost-benefit analysis. Management must look at security with exhaustive due diligence. It must relocate to the Cloud only the information that is not mission critical to the safety and continuity of the business.

[1]Phish—Spam that sends viewer to fraudulent website that looks legitimate and induces viewer to supply confidential information such as passwords and account information.

[2]Pharm—Domain Name Server hacked to redirect traffic to a different site even though it appears to go to the intended web address.

CONFERENCE CALLS
UNLIMITED
MORE THAN A CONFERENCE CALL

Conference Calls Unlimited is dedicated to helping clients worldwide conduct outstanding phone, web and video conferences at fair and economical pricing, combined with unrivaled support.

Sales: 888-901-3471 Customer Service: 877-227-0611

http://www.conferencecallsunlimited.com/