Spring
Professional Leadership Series

Quarter 2. 2013

On Cloud 9: Understanding Cloud Computing

Connecting to the Cloud:
Weighing the Risks and Benefits

Cloud computing is the latest buzzword on the technological front, but it's also one that many businesses approach with scepticism. For some, it just sounds too good to be true — or safe. The perceived risks often overshadow the tangible benefits of low operating and initial setup costs, on-demand resources and unlimited expansion without the need to retool.

New technology makes people nervous. At the same time, declining the opportunity to embrace new technology can leave a company struggling to control costs while clinging to inefficient processes and, ultimately, garnering unsatisfied customers. Cloud computing is an essential leap forward for businesses looking to avoid a budget crisis, reduce costs and generate efficiencies across a decentralised enterprise with separated offices, personnel and clients.

There are some known risks involved with cloud computing, just as there are known risks with outsourcing any data-based responsibility. In this paper, we'll look at the major concerns and separate the fact from the fiction; the hype from the reality. We'll give you the tools to make a decision about cloud computing for a mid-market business based in fact. We'll dispel the rumours and show how your business can maximize the benefits of the cloud while mitigating the risks.

> *"Cloud computing is neither a panacea to cure all business ills or a magic trick comprised of smoke and mirrors. It is a practical business concept designed to relieve some of the problems inherent in today's on-the-go world, freeing executives and employees to reach across borders and barriers, to travel and telecommute, and to get the job done from wherever they happen to be."*

Understanding the Cloud

Most people visualise the cloud in its simplest capacity, as a single entity or a giant, pillowy location stuffed with all the data from all the companies using the cloud. The truth is a little less nebulous and a great deal more practical. It's simply a business model where information and technology is centralised and accessible by any number of communication devices, like smart phones, laptops and iPads, available from any Internet or cell phone connection. For businesses facing budget challenges and employees struggling with workloads, using the cloud empowers fewer employees to manage greater workloads with less stress.

There are three distinct cloud structures in use today:

1 Public Cloud

The public cloud model is shared hosting by multiple customers hosted on a third-party site. One easy-to-understand example is Etsy.com, an online fashion, vintage and antique "mall" where individual store owners upload collections for sale. In this model, each store owner uses the same application platform and is charged only for services used. While the same software platform is shared by all, transactions are exclusive to the mall owner, Etsy.com, and inaccessible by other users. The public cloud is the most cost-effective of the three structures.

2 Private Cloud

A private cloud is comparable to having your company's infrastructure online. Private clouds are almost exclusively used by companies with very deep pockets, as they are usually custom built and often hosted on company servers. This model, which offers the highest level of security, is used by the banking and insurance industries to ensure that sensitive consumer data cannot be breached.

3 Hybrid Cloud

The hybrid cloud model is a combination of both public and private networking using a common management system, where some functions remain in legacy systems and are integrated with other functions pulled from the cloud as shared hosting services. One high-profile hybrid cloud user is NASA's Jet Propulsion Lab. JPL uses multiple cloud platforms in conjunction with its enterprise system to communicate with team members and the public.

For mid-sized businesses, any or all of these models may resolve business issues stemming from overloaded budgets, insufficient staffing and inefficient workload management. Most mid-sized businesses are already feeling the pinch from staff that is stretched too thin over too large a service area.

Obstacles To Cloud Computing — And How To Overcome Them

Over the last few years, the hype about cloud computing has escalated enormously, while in reality only about 20 per cent of businesses have incorporated a cloud model into their business strategy according to a survey conducted in 2010 by IBM — the IBM 2010 Global Risk Survey (IBM)[1] 2010 by Frost & Sullivan. Considering the benefits and savings, this low adoption rate is puzzling. The reason for the gap between hype and adoption seems to be that the cloud concept makes businesses nervous, and while some of that nervousness is based on faulty assumptions, other concerns are valid and deserve forthright discussion. The best approach for businesses is to address these concerns with any potential cloud host and to assess potential risks before implementing a solution.

Let's take a look at potential risk factors and possible solutions. Here are the most common concerns as defined by the IBM survey and suggestions for addressing those concerns.

Security: Threat of Data Breach or Loss

Data security is the number one concern for most businesses, and more than half of business people polled believe that the cloud poses a significantly higher risk. In fact, close to 80% believe that it's more difficult to protect private data in a cloud environment. It's a valid concern; there is an ongoing threat to any shared environment where data may leak out to other cloud users, a malicious cloud user may deliberately hack another account, or an employee of the hosting company may hijack sensitive data. Data transfer may pose vulnerability. However, data isolation failure is a reality under any circumstances, from cloud computing to a briefcase left on a plane.

Addressing the concern —

Reputable cloud providers will offer security solutions like firewalls, secure login and data transfer. Extra security may cost more, but companies only need to pay for enhanced security for sensitive data. They key is in structuring your agreement to protect sensitive data without spending the extra money for non-sensitive materials. In addition, you should find out what kind of backups and assurances the company is willing to offer if there is a breach of security or data loss due to circumstances. Data should be backed up regularly and available instantly. Working with a third party provider may seem riskier, but in reality, data stored on a desktop PC is more vulnerable than an infrastructure designed from the ground up to provide security and backup.

As an additional layer of security, you can associate a strong user authentication protocol to cloud accounts. No data is ever safe if any user's password is "password," or any of the other 100 or so most common passwords used by a majority of the population. A password that is variable length (8-12 characters) and must contain upper and lower case letters, numbers and even special characters, is far more secure than any standard password.

Loss of Control

More than half of IT decision makers expressed concern over third parties involved with sensitive data in a cloud environment. This is more likely to be about security concerns than about territory. It’s not easy to give up control over data security and backup to a third party. Handing data to a provider removes the hands-on nature of being able to personally ensure that the data is handled properly. Transfer of control can make any decision maker anxious.

Addressing the concern —

Unless you are considering a fly-by-night company, this fear is a perceived threat, and the answer is due diligence. Just as you would not invest money in a company without assessing its potential value, you should educate yourself about your chosen provider before taking the plunge. Look at their track record, security and backup protocols, and check out the tools that allow access to the data. Information will foster the trust necessary to move forward.

Application Performance

Just over half of those polled expressed concern regarding cloud-based application performance, which can be affected by a number of factors outside of their control. What if data access is unavailable at a critical time due to server overload?

Addressing the concern —

This is another concern that suffers from worst-case perceptions. No provider can guarantee that their servers will be accessible 100% of the time, but any reputable provider will be able to provide historical data showing server uptime. In most cases, servers may lose connectivity or be overloaded for only short periods of time and statistically, most customers will be unaware, or at worst, mildly inconvenienced. The scenario of your data being inaccessible during the single instant that will make or break your company is a manufactured drama best left to filmmakers. Hire a company you can trust with a history you can verify. Once again, information is the answer.

Vendor Lock-in

About half of the professionals polled expressed a concern that once committed to a provider, they would be locked-in regardless of suitability, and this may be a valid concern. Moving from one vendor to another can be difficult since most cloud providers use a proprietary software platform. A related concern is what happens to the data after a contract is terminated. Will it remain secured and inaccessible to outsiders?

Addressing the concern —

It is true that most cloud providers operate on proprietary software, likely to be incompatible with other systems. This poses a problem when moving data, but it is the same type of problem a business would encounter when moving from one in-house accounting program to another on a desktop computer, or moving from a filing cabinet to digital filing, a situation faced by every medical office in the country over the last few years. Data portability is always an issue, but it is never insurmountable. Ensuring that your data is secure after the contract is terminated should simply be written into the contract. The answer to that concern lies simply in planning ahead for contingencies.

Regulatory Compliance

About one-third of respondents expressed concern about regulatory compliance in a public cloud environment. A large percentage of the people with this concern were in the heavily regulated healthcare and financial services sectors. Compliance can be a tricky issue, and the business, as opposed to the provider, bears the responsibility. The best approach for businesses is to address these concerns with any potential cloud host and to assess potential risks before implementing a solution.

Addressing the concern —

If your company must comply with regulations for secure data handling, make sure the provider you choose is aware of the specific federal and state regulations everywhere you do business as well as where the data itself is located, which may not be divulged as a security precaution. Decide carefully whether a public, private, or hybrid cloud solution best fits your company needs. If budget and data protections are your main concerns, a hybrid solution is usually the best bet, with a private cloud environment for sensitive data and the application code hosted in a shared cloud environment, allowing you to maintain strict compliance while still taking advantage of cost-savings benefits and accessibility.

Developing a Cloud Strategy

Developing a plan for migration to the cloud is as important as developing a plan to start a new business. The best approach is to explore and address any concerns, narrow your provider choice down to a viable candidate and carefully examine your options to assess and mitigate risks. Here are the main points to consider when preparing to migrate to the cloud:

- Migrate data to the cloud on a schedule. Plan ahead. Ask your chosen provider about scalability.
- Follow up. After your data is migrated to the cloud, check with your provider regularly about uptime, backups, and any additional concerns.
- Make your case. Examine the costs, benefits, and risks.
- Choose your provider wisely, based on trust and knowledge.
- Select a plan that offers the appropriate level of security and purchase only the level of security necessary to meet your needs for each function
- Develop protocols for secure user authentication.

No matter how your data is housed, it must be secure. Fortunately, reputable cloud companies are well-versed in data protection.

In most cases, moving to the cloud makes your workforce more mobile and independent, which can represent significant savings in man-hours and hard costs. Cloud computing allows team members to collaborate from multiple locations during any assignment. Paperwork and accounting delays are minimised while reporting and communications are enhanced. Team leaders can use up-to-date field reports to identify potential scope creep well before project costs begin to skyrocket. The result — real-time information accessible on demand — is invaluable to a mid-market business working on a limited operating budget.

Spring
Professional

For More Information:
To find out more about Spring Professional in Asia, or to ask us a question related to this guide, please visit **www.springasia.com**