

10 CONCERNS OF CLOUD COMPUTING

INTRODUCTION:

It's hard to talk to anyone about IT these days without someone mentioning the word 'cloud'. With the concept of externally hosted cloud computing being a buzz concept at the moment many organisations are seeking to reduce cost through use of these new environments. However many organisations fail to look deeper into the cloud phenomenon and see the inherent risk in this new option for organisations finding themselves entangled in regulation and audit failures, vendor lock-in and a reduction in SLA's. The following are nine key factors that any and all professionals need to seriously consider before making the move to the cloud.

CONCERN #1: APPLICATION SUITABILITY

Some applications just don't make sense in the cloud and simply bundling the entire IT operation to the cloud is a risky move. Today the two most successful models of cloud are the elastic LAMP stack model and the batch queuing model most used for digital trans coding. With these models in the cloud it is best used only for non-real-time apps (backups, databases that are infrequently consulted, etc). VOIP, heavy CRM, patient care, ERP and database applications are better suited to the vast majority of users when internally hosted. This approach eliminates concerns about the accessibility, control, availability and stability of mission critical data and applications otherwise questionable when placed within a cloud environment.

CONCERN #2: REGULATION AND LEGISLATION

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. There are issues about laws and privacy which need to be carefully addressed on a case-by-case basis. Potential cloud users need to consult industry regulations and local laws and legislation that may restrict where data can be stored, potentially eliminating the possibility of cloud for many applications and data. Auditors should also be consulted to ensure that future audits will be passed when placing confidential data into a cloud environment.

Possibly even more pressing an issue than standards in this new frontier is the emerging question of jurisdiction. Data that might be secure in one country may not be secure in another. In many cases though, users of cloud services don't know where their information is held. An example of this across common locations cloud storage is used becomes clear when comparing the EU and the USA. The EU favours very strict protection of privacy, while in America laws such as the US Patriot Act invest government and other agencies with virtually limitless powers to access information including that belonging to companies. Following on from legislative issue is that of Sovereignty. When you are in dispute with the service provider any aspect and they won't give your data back, do you know which country's court you are going to deal with them in and what are the laws specific to that legal system?

CONCERN #3: ACCESSIBILITY

The data we store with third parties is accessible not only by us, but by their staff as well. Typical privacy policies grant them permission to work with our data as necessary. While the intentions of any reputable company are good, it only takes one bad apple to sour things. News of inside and outside infiltration is, no matter how rare, bad for business. Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data.

CONCERN #4: NO DISCONNECTED COMPUTING

What happens when the construction company fixing the road cuts your cable connection? Ok, probably the same things as if you used a data centre. But what happens if your cloud is based in the Middle East, or Africa? What happens when a ship's anchor cuts a cable? It could well happen again as it did in Dubai DURING 2008. Most providers won't tell you where your data and applications are sitting so you can never be 100% certain.

CONCERN #5: SECURITY VULNERABILITIES

Let's face it; if you're storing information, you're doing so for a reason. Just as with a local network, the entire chain of security is only as strong as its weakest link. For cloud services, weak links put data at much greater risk of being mined and used by others. In March 2011, marketing firm Epsilon experienced a breach, where millions of names and email addresses were mined from their clients' customer data. From retail stores to banks, hackers got everything they needed to launch widespread spam and phishing campaigns. (Epsilon issued a press release on the matter.)

CONCERN #6: STABILITY

We've all heard stories about businesses being locked out of services: Gmail and Google Calendar outages have become newsworthy events. The inability to access our data, even temporarily, can be significantly detrimental to business. Within Cloud environments outage concerns are clearly a very real and sensible concern. There's no computer network in the world that doesn't have the risk of downtime at some point in its life. However, there's still the ability to receive up-to-the-minute information from an IT department when it's a self-hosted computer network that's at the heart of the problem. What happens, though, when that's taken out into a cloud environment? And, more to the point, what happens when a cloud service a business is relying on goes down, even for a short period? With localised working, even without a network, having some machines with working productivity software installed at least means things can get done.

CONCERN #7: LOSING CONTROL OF DATA

It's not just an emotional attachment to a computer room that keeps companies from outsourcing data. It's the fact that there's an inherent security in having data under close control (assuming there's some kind of remote backup for disaster recovery, of course). Removing the need for local storage clearly has some cost benefits, but for a generation of system administrators and support staff brought up on a different way of working, it's a change that rings some alarm bells. One in particular trusts an external source for working data- what happens if access drops or if someone loses the data as mentioned in other points? Even appreciating the security that cloud computing offers, there's a leap of faith and an element of uncertainty (along with a loss of transparency), that creeps in when data management is moved out of the immediate control of an IT department.

CONCERN #8: THE HIDDEN COST OF THE CLOUD

Cloud services aren't necessarily less expensive. Using hardware and local software to work with data and securely store information can cost less in the long run. Cloud services usually carry monthly or annual fees. Of course, with cloud services there's no maintenance cost for the actual equipment, nor do you pay for software upgrades. But, when you consider the other factors — accessibility, stability, security, and liability — the savings could easily be made up by the business you maintain.

The cost of long-term data storage in the cloud can be compounded when looking at the listed 4 components below and when you consider the data growth rates over the next three years compounded with the increasing retention time of data, the life-cycle cost of data can be really high when you continue to pay for that every month when data is stored in the cloud.

- a. **Data moving costs.** If you have large volumes of data, you can be looking at thousands of dollars for a one-time move from your storage systems to a cloud provider. Much of that charge will come from the bandwidth needs, as many cloud providers will charge upload or download fees. Add in the cost of data growth rates over time and you can be looking at significantly higher fees within just a couple of years. The key is to identify how much data you have to move, and accurately project how much you'll need over an initial three-year period, and factor in those costs.
- b. **Integration costs.** In an internal environment, you can integrate disparate applications in a number of ways (through connectors, third-party apps, or more). In some cases, however, cloud providers don't offer that kind of integration. If they do, you can be sure there's a fee involved. For example, integrating Exchange with a PBX or other phone system may not be possible (or may be very expensive).
- c. **Software testing.** Sometimes, you'll encounter a vendor app that hasn't been run in a cloud environment. You'll wind up putting out time and money if you're using servers or apps that the cloud vendor isn't prepared for.
- d. **Organizational overhead.** When you host an application internally, you may not need to pay for things like facility space or even power needs. Those may be factored into a departmental or organizational structure. When you're relying on the cloud, suddenly you're paying for power or facility rental where previously that was under the auspices of a facilities department.

CONCERN #9: VENDOR LOCK-IN

True standards for how applications communicate and control applications that are in a vendor's cloud have not yet been established. This means that vendors are creating their own proprietary interfaces that could end up tying you to a vendor for longer than you would like. Cloud computing may be erasing the gains we've made in terms of vendor dependence lock-in. Going with a cloud solution means buying into the specific protocols, standards and tools of the cloud vendor, making future migration costly and difficult. The four common types of lock-in are outlined below and should be taken into serious consideration regarding hidden costs and a future lack of flexibility.

- a. **Horizontal lock-in:** This restricts the ability to replace a product with a comparable or competitive product.
- b. **Vertical lock-in:** This restricts choice in other levels of the stack and occurs if choosing solution A mandates use of database X, operating system Y, hardware vendor Z and/or implementation partner S.
- c. **Diagonal (of inclined) lock-in:** This is a tendency of companies to buy as many applications as possible from one provider, even if his solutions in those areas are less desirable.
- d. **Generational lock-in:** This last one is as inescapable as death and taxes and is an issue even if there is no desire to avoid horizontal, vertical or diagonal lock-in. No technology generation and thus no IT solution or IT platform lives forever (well, maybe with exception of the mainframe)

With regards to security when using a cloud service, which of the following concerns you most?

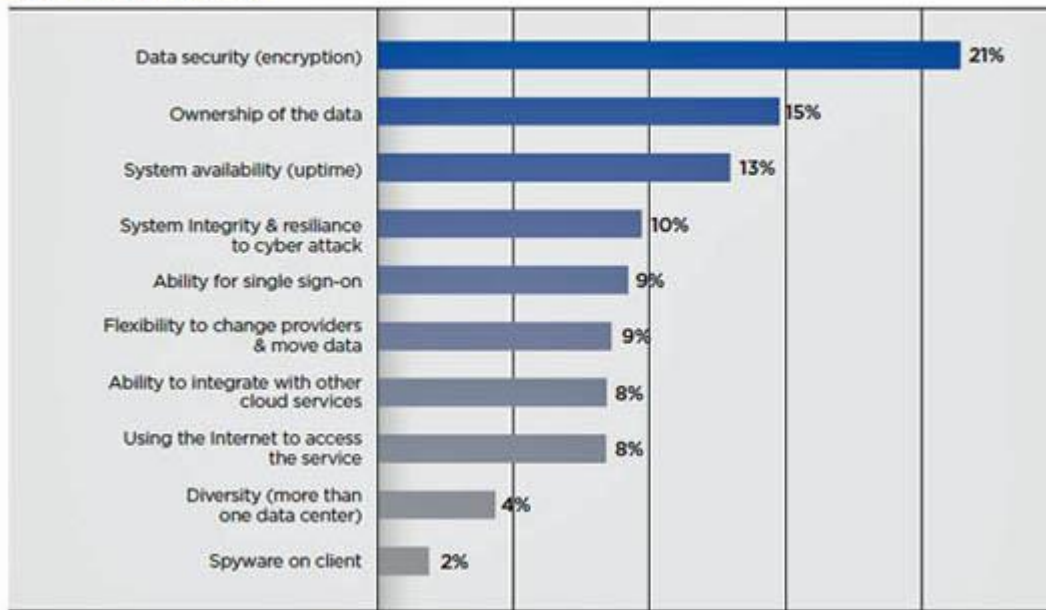


Figure 1.0 – Results of security concern survey as completed by Equinix.

CONCERN #10: REMOVING A SOURCE OF COMPETITIVE ADVANTAGE

You drive a competitive advantage from the IT capabilities you are considering migrating. When you are promising potential clients or presenting members with the exact same promises and SLA's as your next 1000 competitors why would anyone choose you?

SUMMARY:

Cloud Computing is NOT an all-or-nothing decision. There is no valid reason to object to a Cloud migration in block. Rather you should look at ways of combining Public and Private Clouds and identify where it makes sense to deploy Cloud and non-Cloud resources by assessing the needs of each of your company applications.

For any non-mission critical, non-competitive advantage, not complex, not heavily regulated, not sensitive applications and other IT capabilities, Cloud Computing could be the right move. Of course you should always validate the benefits of a cloud migration with a strong business case.

The IT Consultancy Group Pty Ltd (IT Consult)

IT Consult is a full service IT consultancy firm operating out of Sydney, Australia. Whilst specialising in virtualisation IT Consult offers a full range of services to Australia and New Zealand organisations. To contact IT Consult Ph: +61 2 9270 0666 or email: enquiries@itconsult.com.au