Cloud computing - White, Fluffy and Safe or a Hazy, Mysterious, step into the Unknown?

Cloud computing is clearly one of today's most enticing technology areas and is currently one of the top buzzword in the Hi-Tech industry. Cloud computing is not a new concept; most of us already use this technology on a daily basis, through services like Hotmail, Gmail and Facebook. In the simplest of terms, cloud computing is IT-as-a-Service; rather than an organization building its own IT infrastructure to host databases or applications, this is done by a third party with large server farms. The organization then accesses its data and applications over the internet. In other words, under this new procurement model, IT becomes a utility, consumed like water or electricity.

Cloud computing is growing fast, according to Gartner the market is currently worth about $2.4bn, but is predicted to grow to $8.1bn by 2013. Several large companies have already partially adopted the 'Cloud' approach, including all of the top five software companies. More recently business services provider Rentokil Initial has rolled out a cloud email solution to its 30,000 employees.

It's not difficult to see the benefits of cloud computing and enthusiasts are quick to point out its key benefits:

- **Scalability:** Organizations which have grown rapidly, perhaps through acquisitions, often struggle with the complexities required to develop a single coherent enterprise infrastructure. Furthermore, cloud systems are built to cope with sharp increases in workload and seasonal fluctuations. Take for example a tour operator who has to cope with a huge surge in demand during the summer months or a disaster recovery team that requires additional computing power to respond to a large scale emergency.

- **Cost Effective**: As IT providers host services for multiple companies; sharing complex infrastructure can cut costs and allows organizations to only pay for what they actually use.

- **Speed**: Simple cloud services can be deployed rapidly and work 'out of the box'. This is a great advantage for small emerging businesses that may need to establish a secure e-commerce website quickly. Equally, for more complex software and data base solutions, cloud computing allows organizations to skip the hardware procurement and capital expenditure phase.

- **Mobility**: Many companies today operate a geographically diverse workforce. Cloud services are designed to be used anywhere in the world, so organizations with globally dispersed and mobile employees can access their systems on the move.

However, despite the trumpeted business and technical advantages of cloud computing, many businesses have been relatively slow on the take up. Major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. There appears to be significant concerns over certain aspects of cloud computing, including, reduced control & governance, regulatory requirements, excessive standardization, usability and fears over issues of connectivity.

However, without a shadow of a doubt the biggest area of concern is the impact on information security. Will corporate and customer data be safe? What about data protection and legal compliance requirements? What are the corporate risks involved in entrusting a single entity with the data of an entire organization.

Cloud advocates will argue that customers stand to benefit from multiple points of replication and defence and the use of sophisticated technologies that individual companies could not afford; yet others insist that cloud computer is a ‘security nightmare’. Whilst this view may be a little extreme, cloud computing will inevitably have a major impact on the way we think about and react to a variety of information security issues.

For this reason Gartner recently issued a report outlining some of the key information security aspects to be aware of regarding the use of cloud services.

1. **Privileged user access**: Sensitive data processed outside the enterprise brings with it an inherent level of risk, as outsourced services bypass the "physical, logical and personnel controls" in- house IT teams are able to exert. For this reason it is vital for companies to gather as much information as possible about the people who will be managing their data, including the hiring and control procedures of privileged administrators.

2. **Regulatory compliance:** 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. Cloud computing providers must also undergo a similar process before an organization can entrust them with sensitive corporate data.

3. **Data location:** When using cloud solutions you may not know exactly where or in which country your data is hosted. It is important to ask the provider if they will commit to storing and processing data in a specific jurisdictions and whether they will make a contractual commitment to obey local privacy requirements.

4. **Data segregation:** Typically data in the cloud is held in a shared environment alongside data from other customers. For this reason it is important to understand what measures are taken to effectively encrypt and segregate data.

5. **Recovery:** It is crucial for the purposes of Business Continuity Management to understand how your data will be recovered in a disaster situation. Ideally your data and application infrastructure should be replicated across multiple sites. It is also critical to understand the restoration process and anticipated recovery times.

6. **Investigative support:** Investigating inappropriate or illegal activities become significantly harder in cloud computing. The very nature of cloud services makes it especially difficult to investigate a security breach or incident as data logs for multiple customers may be co-located.

Gartner also recommends that smart customers will employ the services of neutral third party, such as Comsec Consulting, to undertake a security risk assessment to map the specific threats and security challenges an organization may encounter upon moving services to a cloud environment. Cloud computing has unique attributes that require undertaking a risk assessment in areas such as, data integrity, recovery, testing procedures, privacy, security policies, in addition to the management, monitoring, alerting and reporting of security vulnerabilities or breaches. It is also important to evaluate the legal ramifications in areas such as regulatory compliance, and auditing.

However, despite some of the security concerns it looks like cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming the fears of the cloud. When considering the solutions to the problems raised by cloud computing, it is important to remember that essentially many of these issues are simply old problems in a new setting. Attacks on server infrastructure and web service vulnerabilities existed long before cloud computing became fashionable. Although some aspects of security will be exacerbated when utilizing the cloud, such as data privacy, segregation, access control and governance, others, such as incomplete security patching, will be mitigated. So whilst cloud computing adds a new dimensions to the security challenge, it also provides an opportunity for improvements.