Managing Cloud Computing Security

Business and strategic decision makers must first evaluate the potential effects of cloud computing on their competitive advantage in order to manage and govern the adoption of cloud technology within an organization. In addition to this, it is also utmost important for any organization to ensure its’ management of Cloud Securities. Here, security becomes one of the important concern as most of the data and computation which were carried out on native machines are now done on remote servers. We can say that security management in cloud is the set of practices undertaken by the firms in order to use their cloud apps and networks to their fullest capacities while minimizing the potential risks and vulnerabilities.

There are certain points which needs to be addressed:

* What steps the company will take to address both new and existing Cloud compliance issues. The potential effects of cloud computing on business in terms of governance and legislation will be covered in this.
* How the use of the cloud computing could impact the organization's business intelligence and intellectual property, potentially affecting how it differentiates itself from competitors.

Senior professionals and management may try to adapt and include current data protection, trust, and privacy rules in setting up a Cloud framework that explicitly targets organizations’ information security in order to create a comprehensive set of Cloud computing standards.

There are certain points which can be included in tightening the security:

* Creating a general business Information protection strategy for cloud computing that demonstrates the organization's position.
* Utilize current TAX and IT audit procedures while including cloud security disclosure and audit procedures.
* When IT decisions are made, they should govern the installation and communication of cloud computing.

Cloud computing guidelines are like a cornerstone of the overall strategy and also focus should be made on Cloud governance and transparency. We must take a note that it is important and essential to provide a framework for privacy within the cloud from the inception.

1. Cloud Governance

In order to safeguard the cloud from potential threats, hackers, and information loss, policies and processes should be put in place. The problem of privacy for software developers is to provide cloud services that reduce privacy concerns and guarantee legal compliance. There are risks related to data storage, distant processing, growing use of virtualization, and platform sharing across users. Concern arises when it becomes unclear to the individuals that why personal information about them is recorded or they are asked to provide and how it will be processed and stored by the other parties. This clearly leads to distrust. The security of data in the cloud is a major worry for consumers, especially in light of the possibility of fraud and financial abuse. Cloud computing may be used securely and confidently once governance and security are in place.

1. Cloud Transparency

Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations [1]. Compared to hybrid or private clouds, public clouds are more likely to be perceived as having a higher level of transparency. This is as a result of public cloud suppliers having "standardized" cloud offerings and hence aiming to attract a larger clientele. Private clouds are typically developed for certain organizations with a greater emphasis on providing customization and personalization cloud capability.

One of the most important protocols in ensuring transparency within Cloud computing is the SLA. The SLA is the only legal agreement between the service provider and client and its importance is greatly discussed in the article titled “Cloud Security Issues” [2]. The SLA is the fundamental mechanism via which the cloud provider can win clients' trust, hence it must be standardised.

The main aspects as a guideline, which the SLA contains, are:

• Services to be delivered, performance,

• Tracking and Reporting

• Problem Management

• Legal Compliance

• Resolution of Disputes Customer Duties

• Security responsibility

• Confidential Information Termination.

One of the main challenges of Cloud computing is that the software vendor should assume responsibility for maintaining the application and ensuring quality of service. [3]

CLOUD COMPUTING’S SECURITY IMPACT

Many users may be unaware that they are actually utilizing an Internet-based service as computer manufacturers, businesses, and colleges roll out cloud-based tools on desktops.

When cloud-based programs lack any recognized browser branding and operate even when the user is not connected to the Internet, the danger of confusion is likely to increase. When signing on to access data utilizing cloud computing, HTTPS and WS Security should be used as a minimum. WS-Security assists with SOAP messages by defining the header that carries the WS-Security extensions. Additionally, it defines how existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages [4]. Thus far there has been four service failures identified between Amazon and Google in 2008, ranging from 1.5 to 8 hours downtime. Organisations must decide whether proper security measures are in place (to secure their data and applications) or do they share a joint responsibility with service providers when engaging in the cloud environment [5].

In the book titled ‘The Tower and the Cloud’, Richard Katz focuses on many areas where the cloud may impinge on education [6]. He argues that businesses should be concerned about what might happen to the information because they may be storing papers that shouldn't be made public. Moving toward a single cloud interface may make it simpler for attackers to endanger clouds, thus prospective cloud organizations and vendors need to be aware of this possibility.

[1] Brodkin J, 2008, ‘Gartner: Seven cloud-computing security risks’, Infoworld, viewed 13 March 2009, from

<http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1>

[2] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, ‘Cloud Security Issues’, 2009 IEEE International Conference on Services Computing, viewed 26 October 2009, pp 517-520.

[3] ] S. Arnold, 2009,’ Cloud computing and the issue of privacy’, KM World, vol July/August 2008, www.kmworld.com, viewed 19 August 2009, pp 14-22

[4] Gruschka N, Iancono LL, Jensen M and Schwenk J, ‘On Technical Security Issues in Cloud Computing’, ‘09 IEEE International Conference on Cloud Computing, pp 110-112, 2009.

[5] Armbrust M, Fox A, Griffith R, Joseph D A, Katz H R, Konwinski A, Lee Gunho, Patterson A D, Rabkin A, Stoica A, Zaharia M, (2009), Above the clouds: A Berkeley view of Cloud Computing, UC Berkeley EECS, Feb 2010

[6] Goldstein, P (2009), The Tower, the Cloud, and the IT leader and workforce, in Katz, R (ed) (2009), The Tower and the Cloud: Higher Education in the Age of Cloud Computing, Educause http://www.educause.edu/thetowerandthecloud