Chapter 83
Organizational Control Related to Cloud

Sathish A. Kumar
Coastal Carolina University, USA

ABSTRACT

Cloud computing is touted as the next big thing in the Information Technology (IT) industry, which is going to impact the businesses of any size. Yet, the security issue continues to pose a big threat. Lack of transparency in the infrastructure and platforms causes distrust among users, and the users are reluctant to store information on the cloud. This undermines the potential of cloud computing and has proved to be a big barrier in the realization of the potential of cloud computing and its widespread adoption. The big paradigm shifts in the technology has not been reflected on the methods used to secure the technology. When an organization builds the infrastructure for cloud computing, security and privacy controls should be kept in mind from the holistic security perspective. It is also critical that the organization monitor and adapt controls to determine the success of cloud computing in dealing with the security and reliability issues relating to the cloud. From an organizational control perspective, the authors suggest an independent governing body to mediate between the cloud provider and the user, with the control framework that they have developed to fulfill their responsibilities of protecting the cloud environment.

1. INTRODUCTION

National Institute of Standards and Technology (NIST) defines cloud computing as a computing model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) (Mell, 2011). These services can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST also defines that the cloud computing can be achieved through three service models: *Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).* Cloud computing can be implemented by the four deployment models: *Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud.*

Cloud Computing is widely considered as the next big thing in IT evolution, and is getting rapid adoption in the industry. This emerging paradigm allows an organization to reduce costs and develop highly scalable solutions (Armbrust, 2009). Cloud promises customers with the benefits of a more

DOI: 10.4018/978-1-4666-6539-2.ch083

convenient way of provisioning IT resources at a faster speed and with a lower cost, compared to traditional IT processes and systems. Cloud Computing provides the following important features (Sarna, 2011).

Availability: Services of Cloud Computing are ubiquitous and can be accessed from anywhere and by anyone just by signing in. Due to high availability, large amount of data can be uploaded and retrieved from the cloud. This data can be accessed from any devices - laptops, desktops, mobile phones, tablets etc.

Scalability: Depending upon number of users logged in or the amount of data accessed, the number of servers can be increased or decreased in order to handle the demand through regular monitoring of the systems. The scaling is done with the help of Virtualization. Virtualization is achieved with the help of hypervisors such as VMware vSphere, Citrix XenServer etc.

Low Cost: Small companies and startup companies that are in the early stages of their inception find cloud computing a very efficient way to set up the Infrastructure. This is due to Infrastructure as a Service (IaaS) offered by Cloud Computing which provides an infrastructure to companies. Therefore the companies need not set up the infrastructure themselves. They can just get a monthly or annual subscription of a Cloud Server on a pay-what-you-use basis. That way the businesses don't need a huge IT investment upfront and can scale their IT budget up and down based on the business demand. All these advantages seem to be very enticing and as a result cloud computing has become very popular in recent years. Due to this, more and more IT resources, such as software, platform and infrastructure are available on the cloud and subsequently, it results in more risk factors. There are more attackers that have become active, for example active Denial of Service (DoS) attacks on the cloud providers such as Amazon, Yahoo and Google. Thus, Cloud computing has proved to be a very promising field with many benefits but the major problem that remains is of security and compliance with regulations regarding privacy.

Users generally do not rely on cloud service providers on whether their data will remain secure or not. Cloud service providers are reluctant to provide information about how they keep the data and geographical locations of their data centers. This is very obvious as it helps them keep the data safe and away from the eyes of the attackers. This in turn causes distrust among the users as they do not know where their data is and whether it is secured or not. They cannot just blindly trust the techniques used by cloud service providers without actually knowing them. As a result, users are hesitant to put their valuable and confidential data on the cloud as it may reduce the confidentiality of their data and may result in their private data becoming public. This is resulting in undermining the potential of cloud computing and making its growth slow down a little.

Cloud service providers try to provide cloud services with built-in security features. They try to build a cloud infrastructure that can withstand any sort of failure whether it is technical, logical or physical. However, there are many factors that can harm the security and reliability of the Cloud infrastructure despite of taking all the necessary steps. There are generally categorized in the following three layers, in which an organization takes control of the security. These are as follows:

- **Physical Layer:** The physical layer of security encompasses many factors.
    1. **Data Center:** This deals with the geographical location of the data center. Locations are chosen in such a way that they are not prone to natural or man-made disasters. No data center will be successful in withstanding severe earthquakes, cyclones, volcanic eruptions etc. and it is best to keep the data center in a place that is less vulnerable to be affected by these factors. Also, location of data centers is kept