Chapter 79
Risk Management in the Cloud and Cloud Outages

S. Srinivasan
Texas Southern University, USA

ABSTRACT

Cloud computing is facilitated often through the open Internet, which is not designed for secure communications. From the cloud user perspective, access to the cloud through a Virtual Private Network (VPN) is a possibility, but this is not the default access method for all cloud users. Given this reality, the cloud service users must be prepared for risk management because they do not control the cloud hardware or the communication channels. Added to this uncertainty is the potential for cloud service outage for risk management planning. In this chapter, the authors discuss the various aspects of risk management from the cloud user perspective. In addition, they analyze some of the major cloud outages over the past five years that have resulted in loss of trust. This list includes the outages in Amazon Web Services, Google, Windows, and Rackspace.

1. INTRODUCTION

Cloud computing is designed to operate over the internet. The internet is not designed with security in mind. All cloud users when they give up control over their hardware, software and data still have the obligation to protect the security of their data. Any loss or compromise of their data will result in major business consequences. Added to this uncertainty is the loss of access to their information systems because of outage at the cloud service providers. In the case of major providers such as Amazon Web Services, Google and Rackspace the outages are rare. By the same token, any brief outage in the availability of cloud services is a major problem for the cloud customers. Major cloud service providers build-in various layers of redundancy in storage as well as computing power. Yet, sometimes they fail in their efforts to provide uninterrupted service. Over the past five years there have been several well publicized outages of cloud services. Our goal in this chapter is to analyze the risk management aspects in the cloud and connect it with how cloud outages erode trust among users.

The risk management concept requires the user to control the resources that they are trying to use and protect. The research literature discusses risk

DOI: 10.4018/978-1-4666-6539-2.ch079

management from various perspectives. The core of cloud computing relies on resource sharing and multi-tenancy. This means that the cloud service provider such as Amazon is able to provide service to numerous customers using large servers. Major risk factors arise when there is multi-tenancy because data belonging to one customer could accidentally be accessed by an application running on another customer's virtual server. One obvious solution is to limit multi-tenancy. It is not possible for majority of cloud users. The concept of Virtual Private Cloud (VPC) provides a solution for this risk factor but it is an expensive solution. Moreover, it defeats the economies of scale that the cloud offers in keeping the cost low for many cloud users. The risk management applies both to the cloud user and the cloud provider. The cloud provider aims to bolster trust among its users by putting in place mechanisms that lead to compliance certification from external agencies such as SAS70 Type II Audit compliance, FISMA, and PCI-DSS compliance.

Gartner's report points out that a major source of risk for customers stem from Software as a Service (SaaS) application (Gartner Report, 2013a). When customers contract for this type of service they are dissatisfied with the level of guarantee on data protection that the provider is able to offer. The major risk for the cloud customer comes from the data comingling aspect. Moreover, the outages in the provider services lead to lack of trust. To overcome these concerns the cloud service provider should be able to provide the cloud customer with an annual audit of their security practices and third party validation of their controls. Another important data that the cloud customer could use comes from the Cloud Security Alliance's recommendation for a Cloud Controls Matrix that the provider could share with the customers. The Cloud Controls Matrix contains recommended goals for risk management from several cloud customers.

2. RISK MANAGEMENT

Risk is defined as the likelihood that an event will occur that affects the ability to achieve certain goals. With this definition of risk, we can classify the risks as pertaining to system availability, data integrity, system performance and security in general. When a customer uses a cloud service their major risk is with respect to the cloud system availability. In the next section we have addressed some of these aspects to show certain metrics that the customer can evaluate about the service provider's obligations for system uptime. When the service provider is unable to maintain the level of uptime promised then it leads to multiple risks for the customer. Risk management involves having processes to handle these types of risks.

From the customer perspective, managing the risk associated with system availability involves using more than one cloud service provider. For example, the customer could use one cloud service provider for all primary functions but use another service provider for cloud backup. This way, when the main service provider's system is not up then the customer could access their data from the other service provider where the backup data is stored. Theoretically this is feasible but from a practical perspective it is more complex and expensive. The customer must have a way of disk mirroring all activities on the main service provider's system onto the backup service provider. One way to handle simultaneous storage of data among two different providers is to use a peering system. Such solutions exist but are often too costly for most organizations.

Cloud customers evaluating risks should consider four aspects with respect to risk management. These are: Avoidance, Mitigation, Sharing, and Acceptance. Avoidance requires the customer to take prudent steps to avoid the risk. With cloud computing, the choices available to the customer are either very minimal or costly. In many cases