Implementing COSO ERM Framework to Mitigate Cloud Computing Business Challenges

Khaled Almgren
PhD Candidate
Computer Science and Engineering
School of Engineering
University of Bridgeport
126 Park Ave
Bridgeport
CT 06604

Abstract

Cloud computing can be defined as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction. Despite the many benefits that such a process confers to a business entity, there are several challenges that have discouraged its adoption among business entities. Most of them are mainly with regards to the privacy and confidentiality of data, data theft, and threat to continuity of business. Using COSO-ERM integrated framework, an organization can be able to come up with a reliable response to the various threats posed by these risks. A survey carried out on the acceptability of the COSO ERM framework by managers of various business entities showed that the framework could be widely accepted by various organization as a means of managing various risks associated with the adoption of cloud computing. 86 percent of the respondent agreed that the framework could provide a reliable solution for organizations looking for a reliable risk response plan.

Keywords: Cloud Computing, COSO-ERM, Integrated Framework, Computing Resources

Introduction

Cloud computing can be described as the movement of various applications into the internet and a considerable increase in the use of internet to acquire a certain service that was traditionally accessed from a company's data center (Creeger, 2009). As such, it can be described as delivery of various computing services over the internet, which allows various individuals and businesses to use various software and hardware that are maintained by a third party in a remote location. This includes computing services such as storage of files, webmail, online business applications, and social networking sites (Sotomayor et al, 2009). Cloud computing ensures that information can be accessed from anywhere so long as internet connection is available. Cloud computing avails shared pool of resources for an organization including data storage space, networks, computer processing power, and specialized applications for the computer as well as the various users. Despite this cloud computing also presents several challenges for a business making it difficult for most organizations to adopt use of cloud computing. This can be solved by adopting a COSO-ERM risk management framework in dealing with the various threats that are likely to be encountered by a business adopting use of cloud computing. This paper looks at cloud computing and describes a solution that could be effectively applied to deal with these challenges.

Literature Review

There is no definite information discussing the origin of the term of cloud computing and there are several suggestion as to the origins of the term. According to Bartholomew (2009) suggest that the term cloud computing can be attributed to Eric Schmidt in 2006 whereas Kaufman (2009) points out that the term can be traced to 1990s when various providers started using Virtual Private Network (VPN) services for data communication. However, there is an agreed definition of the term cloud computing as suggested by National Institute of Standards and technology.

Cloud computing is defined as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction" (Mell 2009, 9). It is delivered in various architectural types and models and offers various advantages to a business organization.

The intake of cloud computing by various business organizations has been hindered by various threats that are associated with the adoption of cloud computing. According to Ristenpart et al (2009), an organization exposes itself to various attacks targeting shared-tenancy environment. Cloud computing involves use of a single physical machine through the use of virtual machine software implementation. This implies that data from different clients is hosted on separate virtual machines but are al kept in a single machine located in one place. A study conducted by a group of computer scientists from key universities; Massachusetts Institute of Technology and University of California found that it was possible for a hacker to infiltrate the virtual machines so as to gain access to the physical locations of the virtual machines. In the study, the scientists were able to load eavesdropping software onto the servers that were hosting the websites that they were targeting. This attack is regarded as the side channel attack and it is usually presents a possibility that an organization can lose its key information as a result of adopting use of cloud computing in its operations (Hardesty 2009).

A second business challenge that stunts the adoption of cloud computing in businesses is threats posed by malwares that may be used by an attacker to exploit the vulnerabilities that may be present in various virtual machines. Keizer (2009) observes that malicious codes can be designed in such a way that they infect both the physical and virtual machines. This can be achieved by use of various cloaking technologies that hides some of the key components of the computer from being checked for security by security maintenance software in a machine such as antivirus. Price (2008) observes that the VM-based toolkits could be used by various attackers to help them gain the access of an operating system without the operating system recognizing that it has been compromised by the toolkits. Once there, the toolkits are able to control all the key hardware interfaces, enabling them to acquire data that may be used by the hacker to gain control of the primary host.

Another key challenge that makes adoption of cloud computing a challenging business endeavor is the state of regulation and governance of the cloud computing services providers. To a large extent, the level of privacy and confidentiality of the services offered by the various providers of the services are largely dependent on the terms that are agreed between the clients and the cloud computing services providers. Gellman (2009) observed that the risk posed to the confidentiality of the data as well as the privacy of various information can be largely increased when the cloud provider reserves the right to change the terms and policies of the agreement at will. As such, businesses are cautious when entering into agreement with the cloud providers to make sure that the privacy of their information and data is highly guaranteed by the cloud providers. It is always poses a huge challenge for a client accessing cloud services to determine the jurisdictional law which binds a cloud provider making it difficult to determine if cases of loss of privacy and confidentiality due to actions of the cloud provider can make the provider liable for the damages caused to the business.

Espionage threats also present a significant challenge to various businesses that intends to take up cloud computing. Helft and Markoff (2010) observe that various countries are investing heavily in making sure that they have various agencies that have cyber-offensive capabilities. This implies that the next wave of attacks may be highly targeted to various businesses that have taken up cloud computing as a part of their operations. There is increasing chances that foreign intelligence will use their cyber threat capabilities to store information from various organization that have integrated cloud computing as a key part of the business operations. Gellman (2009) observed that there is also a huge possibility that the providers of cloud services will be required by various organizations to scan information stored by various organization in their servers for information that they believe may be a threat to national security. In case where overseas cloud providers are involved in the sharing of client information, the law may not oblige them to report such information to the businesses. As such, this is discouraging various organization from adopting cloud computing as they are wary of various threats posed by increased government investments in cyber-security as well as in dealing with various challenges that they consider to be important to national interests.

Finally, another key challenge that is making it hard for various business organizations to adopt cloud computing in their operations is the threat that is likely to crop up as a result of disruptions in the internet services. Metz (2009) observes that adoption of cloud computing by a business entity implied that such an organization exposed itself to possibility of disruption of business activity where the cloud provider is taken offline.

Metz observes that it is possible to take the cloud servers offline by using various denial of service attacks. There are substantiated concerns that the continuity of business may also be affected in cases where the policemen seize the physical machine that hosts the virtual machines. This would imply that all the virtual machines that may be hosted in the physical location may all cease to function until such machines are returned. This may threaten the continuity of the business especially where the key functions of the business are stored in the virtual machines. This makes it hard for the businesses to view adoption of cloud computing as a viable option for them since they are aware that there may be challenges with the continuity of the business.

Given these highlighted challenges that a business is likely to face as a result of adopting cloud computing, it is important for an organization to have a risk management plan in place to make sure that they are able to deal with these threats.

Problem Statement

Despite the benefits that are associated with cloud computing, most businesses are not enjoying these benefits as they are not sure of how they can be able to mitigate the effects of these threats to their businesses (Everett, 2009). As such, there is need to adopt a risk management tool that can be used to deal with these threats as well as identify the effectiveness of adopting such a tool to some of the businesses that have adopted such a tool.

Proposed Solution

The key solution that can be used by various organizations in order to deal with the various challenges that are involved in cloud computing is use of the integrated COSO-ERM framework to come up with reliable responses to deal with the various risks that are associated with the adoption of cloud computing within an organization. This is a risk management tool that is highly effective in identifying various risks and coming up with the applicable responses that can help the organization to deal with them. In essence, it allows an entity to respond in a manner that reduces the likelihood of downside outcomes and increases the potential for upside outcomes.

Objectives and Benefits of COSO ERM Framework

There are several benefits and objectives that are associated with use of COSO ERM framework in assessing the threats posed by various risks. First, the framework helps in aligning risk appetite with the strategy of the business. This is done by determining the degree of risk than an entity is willing to accept in pursuit of its goals. Second, the framework helps in linking growth, risk and return. As such, COSO ERM provides an enhanced ability to identify risks, assess them and establish acceptable risk relative to growth of return objectives. Third, the framework enhances risk response decisions as it allows an entity to identify and select among alternative risk responses; risk avoidance, reduction, sharing and acceptance. Fourth, the framework minimizes operational surprises and losses as entities are given the means by which they identify potential events, assess risk and establish responses. This reduces the occurrence of surprises and related costs or losses.

Fifth, the framework makes it possible to identify and manage cross-enterprise risks by helping management not only to manage individual risks, but also to understand interrelated impacts. Sixth, the framework provides integrated responses to multiple risks by enabling integrated solutions for managing an entity's many inherent risks. Seventh, the framework enables an organization to seize opportunities. Management considers potential events, rather than just risks. Therefore, an entity gains an understanding of how certain events represent opportunities. Finally, the framework enables an organization to rationalize capital. Detailed information on an entity's total risks allows management to more effectively assess overall capital needs and improve capital allocation. As a result of the many benefits of this process, the COSO ERM has been selected as a solution for dealing with challenges facing businesses that intends to adopt cloud computing (COSO, 2004).

Methodology

The three key processes that are involved in risk management using the COSO-ERM framework are event identification, risk assessment, and risk response development (Moeller, 2011). The event identification involves putting down all the key risks that a business is likely to be faced by their in their decision to adopt cloud computing. In this case, all the key risks have been identified in the literature review section. After event identification, the amount of risk posed by each of the risk is then assessed. This is done by examining the implications of a certain risk and how it is likely to affect the performance of an organization.

In order for the COSO ERM framework to be effective, risk assessment criteria must be developed before the risk assessment process starts. The same common criteria must be used by all business units, corporate functions and large capital projects. Using the same scale across all business units helps to ensure consistency within the process. The scales should have the right balance between simplicity and precision. The staff members using the scales should be able to assess risks without wasting time on immaterial decisions. All of the risk events that are identified are supposed to be assessed using the same impact and likelihood scales.

The impact scale represents the extent to which an event would affect the enterprise as a whole. A variety of impact assessment criteria was used when developing the scale and including, financial, reputation, safety, employment, regulatory and other considerations. Risk assessment is useful in determining the risk appetite of an organization.

After the assessment, risk response plan is developed by the management to deal with various risks that are identified in the risk assessment process. The responses are then notified to all the key employees and the various key responsibilities that they are supposed to play are well communicated.

Experiment

In order to establish the applicability of the suggested solution, it was important to carry out a survey to determine if the developed solution would be effective in dealing with the business challenges that were making it hard for businesses to take up cloud computing. A survey targeting the manager of various middle sized business were targeted and given a comprehensively prepared COSO-ERM framework that addressed all their key challenges. They were supposed to review the framework and then a survey (see Appendix 1) was taken to establish whether they were confident in the ability of the framework to deal with their various concerns.

The survey showed that 86 percent of the interviewed managers were highly satisfied with the framework and were confident that their business entities could use the framework to mitigate the effects of the various risks that were likely to result as a result of their decision to adopt cloud computing. 3 percent of these managers claimed that they would improve on the provided framework to include several other risks that were not covered in the framework. However, 14 percent of the surveyed managers claimed that they were not very sure about the ability of the suggested response to deal with the challenges that they expected from the adoption of the cloud computing.

Conclusion

The results of the experiments showed that most of the challenges that were being faced by the managers in the decision to adopt cloud computing. Most of the managers were aware of the significant threats that comes with adoption of cloud computing. There are many challenges that occur as a result of cloud computing. Most of them are mainly with regards to the privacy and confidentiality of data, data theft, and threat to continuity of business. Using COSO-ERM integrated framework, an organization can be able to come up with a reliable response to the various threats posed by these risks. A survey carried out on several manager of middle sized businesses observed that the framework could be effective in dealing with the various challenges associated with cloud computing.

References

Bartholomew, D. (2009). Cloud rains opportunities for software developers. *Dice* 29 May. http://careerresources.dice.com/articles/content/entry/cloud_rains_opportunities_for_software

Creeger, M. (2009). CTO roundtable: Cloud computing. *Communications of the ACM* 52(8):50–56

COSO, I. (2004). Enterprise risk management-integrated framework. *Committee of Sponsoring Organizations of the Treadway Commission*.

Everett, C. (2009). Cloud computing—a question of trust. *Computer Fraud & Security* June: 5–7

Gellman, R. (2009). *Privacy in the clouds: Risks to privacy and confidentiality from cloud computing*. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Hardesty, L. (2009). Secure computers aren't so secure. *MIT press release* 30 October. http://www.physorg.com/news176107396.html

Helft, M. & Markoff, J. (2010). In rebuke of China, focus falls on cybersecurity. *NYTimes* 4 January. http://www.nytimes.com/2010/01/14/technology/14google.html

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security & Privacy* July/August: 61–64

Keizer, G. (2009). VMware bug allows Windows hack to attack Macs. *Computerworld* 16 April. http://www.networkworld.com/news/2009/041509-vmware-bug-allowswindows-hack.html

Mell, P. (2009). *Effectively and securely using the cloud computing paradigm*. http://csrc.nist.gov/groups/SNS/cloud-computing/cloudcomputing-v26.ppt

Messmer, E. (2009). Gartner on cloud security: 'Our nightmare scenario is here now'. *Computerworld* 22 October. http://www.networkworld.com/news/2009/102109-gartner-cloud-security.html

Metz, C. (2009). Bitbucket's Amazon DDoS—what went wrong. *The Register* 9 October. http://www.theregister.co.uk/2009/10/09/amazon_cloud_bitbucket_ddos_aftermath/

Moeller, R. R. (2011). COSO ERM Framework. *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes, Second Edition*, 51-87.

Price M (2008). The paradox of security in virtual environments. *Computer* 41(11): 22–38

Ristenpart T, Tromer E, Shacham H & Savage S (2009). *Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds*, in proceedings of the 16th ACM conference on Computer and communications security, 07. New York, NY: ACM Press: 199–212

Sotomayor B, Montero RS, Llorente IM & Foster I (2009). Virtual infrastructure management in private and hybrid clouds. *IEEE Internet Computing* 13(5):14–22

Appendix 1: Survey Questions

Business name:
Position held:
Have your entity adopted cloud computing?
Yes
No
If not, does your entity intend to adopt cloud computing?
Yes
Maybe
No
In your opinion what is the largest challenge faced by business adopting cloud computing?
_____
Do you think the benefits of cloud computing outweighs the challenges
Yes
Maybe
No
What do you think of COSO ERM framework?
_____
Do you think the COSO ERM framework will be effective?
Yes
Maybe
No
Would you use the framework for your organization?
Yes
Maybe
No
If not, what aspects of the framework would you improve?
_____

Appendix 2: COSO ERM framework