HANIF SHAMJI, MBA, CPA, CGA
CHARTERED PROFESSIONAL ACCOUNTANT
FINANCE BUSINESS PARTER -
OPERATIONS AND STRATEGY PROFESSIONAL

Cloud Computing Security Concerns – April 3, 2017

What is Cloud Computing

Cloud computing allows users to access software and stored information from the internet without having to have software or data stored on their computer. It allows users to access information through a computer, tablet, or smartphone either from an app or through a web browser.

It has the potential to allow organizations on limited budgets access computing at lower costs. It also allows for more flexibility in allowing information from different sources to be presented in a coherent manner. Because of the flexibility, it allows organizations to access information from a variety of devices. Also, cloud computing can be seen as outsourcing some of the organizational IT services to a third-party provider, thereby allowing it to focus on its core competencies.

There are advantages to cloud computing including flexibility, cost control. Cloud computing can be done through a third-party provider, in-house, or a combination of the two. Having up-to-date patient information on tablets when reviewing patient files can increase efficiency. As well salespersons can have up-to-date information related to their customers including concerns which they can address.

Understanding Cloud Computing Before Committing

It is important to understand cloud computing from an organizational strategy standpoint and a security standpoint. We sometimes hear account sales managers from various cloud providers or CRM solutions promote their product without really understanding the product itself. The question to ask does account manager understand what cloud computing is, the product and common security issues or are they merely focusing on their quarterly commission or bonus targets. It is important to understand the fundamentals of cloud computing, as well as beware of concerns that the sales account manager should be able to address appropriately. If you are not able to get a satisfactory answer you should ask do I have the right contact person, or is this the right service provider for the organization.

Before committing to any cloud solution concerns related to information strategy as well as information security should be addressed upfront. An understanding of the terms and conditions including exit clauses should be well documented including access to organizational information if service is discontinued.

Advantages to using the Cloud

Adopting cloud computing has some advantages including reduced cost of ownership. An organization that has limited resources, is in growth mode or does not require a dedicated application can benefit. It also allows for flexibility when implementing applications as IT operations are outsourced. It also allows organizations to have a competitive advantage by flexibility to scale as an organization grows or expands in other industries.

Challenges to using the Cloud

However, cloud computing is not without concerns which include security, service outage, and disaster recovery to name a few. Local statutory requirements may also dictate that data be stored, or not stored in certain locations which should be addressed.

Consider how an organization will continue its operations should internet connectivity go down or the service provider's site goes down. Who is responsible for information stored on the service providers site, and is an independent audit conducted to ensure that information is secure, reliable, and the service is stable. Understand terms of the agreement related to the responsibility of the service provider, and the organization.

Access to Information

An evaluation of internal controls related to access to information will need to be undertaken including access to information, regulatory compliance, financial internal controls, segregation of duties and access, monitoring of activities to detect and prevent unauthorized access, as well as the recovery of information.

The cloud has become host to a variety of documents ranging from personal documents, banking information, corporate information including proprietary information. There have been cases where data was compromised from organizations where it can have an impact on the goodwill that has been built, future profitability, as well as legal challenges related to the compromised data. Regardless of the cloud topology, information security is a concern that should be addressed.

Need for Security Related to Cloud Storage

Data loss and unauthorized access are often seen as a major challenge. This risk can be mitigated through the use of encryption protocols, redundant data storage, as well as ensuring the implementation of internal controls related to the storage of data. Another threat is the possibility of data that is deleted without a trace from the information system. This might be due to careless storage procedures by the cloud provider, or a malicious hacker targeting the service provider or your organizational information. Information attacks could also involve eavesdropping on organizational operations through the information it stores. Consider the potential risk to the organization, and the clients it services. This could be done through a direct hack or redirecting your clients to their website to obtain client information.

An organization could also be hit with a denial of service That could stop an organization from accessing information on the cloud or reduce access thereby reducing the efficiency of the use of the cloud. Insecure applications interfaces and protocols can lead to an access point for third parties to access the information either directly or through intercepting information.

Cloud Service Provider Obligations

Review the terms of contract with the service provider related to how security issues are dealt with, what the provider is doing to ensure security as well as their obligation, as well as that of the organization. A review of the terms of service should be undertaken to ensure that it adheres to best practices related to information security. A review may include visiting the cloud computing

site to determine security protocols, an organization may use third party security professions if it does not have the necessary resources. Ensure that the responsibilities of both the service provider and the organization are clearly outlined in the terms of contract in order to reduce any misunderstanding.

Obligations of the Organization

Ensuring security does not only rest with the service provider. Organizations need to ensure that proper internal control policies and procedures are adhered to. This including ensuring that proper internal controls are in place which includes ensuring proper access controls, segregation of duties, protecting passwords, as well as ensuring security patches are up-to-date.

The obligations to security are not reduced due to the fact cloud computing is used. A malicious insider such as a disgruntled employee could also pose a threat this includes downloading sensitive customer information. Proper physical, and electronic security control policies and procedures should be in place and enforced. Access controls should be granted and revoked on a per-need basis. As well regular internal control checks both from an information control and financial control standpoint should be undertaken.

Best practices such as ensuring strong encryption for data that is stored on the organization's systems, ensuring proper control protocols per best practices. Organizations are responsible for ensuring information security not only the cloud provider. Well documented policies and procedures related to the access of information, usage, and storage should be in place.

Policies should be well understood, and routine audits should be undertaken to ensure compliance. A one size fits all policy cannot solve security issues. Security is a shared responsibility amongst all stakeholders.

Types of Clouds & Cloud Models

It is important also to understand the various types of clouds and cloud models. The security issues that surround it. While the detailed security issues will differ by the cloud topology the fundamental security issues remain related to information security. The challenges may be complex depending on the type of cloud, or combination of clouds that are used.

Types of Clouds

IaaS – Infrastructure as a Service – this type of cloud infrastructure typically allows organizations to run their software on various hardware from the cloud provider

PaaS – Platform as a Service – This offers a development platform which includes an operating system, and programming language.

SaaS – Software as a Service – Allows users to applications via the internet, which may be based on a usage-based, or per user base.

Typical Cloud Models

Private Cloud – solely used by an organization which is managed internally, or by a third party

Public Cloud - Services on a network that is open to the public

Community Cloud – Shared amongst several organizations

Hybrid Cloud – is a combination of two or cloud models

Conclusion

Cloud computing has security challenges ranging from traditional physical internal controls to those related to information security both from internal and external access it does offer advantages. The security controls cannot be ignored as it could affect an organization's statutory requirements, lead to the loss of competitive information such as customer information, or patents.

Cloud computing offers advantages including scalability for organizations that do not require a dedicated cloud service. It also can provide the flexibility to allow for organizations to tailor the usage to requirements. As well it can be a focal point for combining information from various sources that may be used for strategic decisions.

While cloud computing has its challenges, and benefits the use of cloud computing should not be dismissed or embraced fully without addressing concerns related to information security and service contracts. With dependence on information security throughout the organization the importance security compliance in order to comply with national, or industry best practices should be undertaken.

About the author:
Hanif Shamji, MBA, CPA, CGA is a Finance Business Partner / Sr. Financial Analyst with an information technology background, experienced in several industries.
Contact: info@hanifshamji.ca
http://www.hanifshamji.ca/