Whitepaper: Security in the Cloud

Security in the Cloud: Visibility & Control of your Cloud Service Providers

Date: 11 Apr 2012

Doc Ref: SOS-WP-CSP-0412A

Author: Pierre Tagle Ph.D., Prashant Haldankar, Murray Goldschmidt

Table of Contents

Overview

The deployment to the Cloud is dramatically on the rise as organisations look beyond the hype and adopt this technology based on its current maturity. This year 80% of Fortune 1000 enterprises will pay for cloud computing services, and 30% will pay for a cloud-computing infrastructure [1]. Interestingly, at the same time, the technology will reach the mainstream and soon after become the desired choice for the majority for application development efforts amongst large enterprises [2].

The objective of this whitepaper is to establish a security context to hosting services so that the reader can make an informed decision in selecting a Cloud Service Provider (CSP) to deliver their service requirements. An overview of benefits offered by CSP's is provided along with the key risks and challenges in adopting such services and also addressing an organisation's security requirements.

A list of questions is provided to stimulate thought around topics that may influence the security of a hosted solution. Whether an organisation has existing hosting arrangements or is considering embarking on this journey, the information presented in this paper should put the reader in a position to objectively make an informed decision regarding their entry into the Cloud and their relationship with the CSP, or review and reconsider existing arrangements.

The practice of outsourcing the management and hosting of business processes/applications and infrastructure is widespread across many industry sectors including government, public and private education and commercial entities. The cloud model is a particularly appealing service offering where organisations have either limited capability in-house or require specific availability, throughput and data requirements that cannot be delivered economically from their own facilities. IT services for the delivery of business processes through a CSP could range from infrastructure services for hosting server environments to extensive enterprise type applications made available to the organisation as a managed service.

From a business perspective, CSP offers the ability to adopt the latest technologies in a pay-as-you-go model that delivers the cost benefits of variable pricing without a costly investment in hardware and software. From an IT perspective, the cloud provides an infrastructure and application models that can be rapidly provisioned and released to keep up with the ever changing business and consumer demands. In combination, it is evident that CSP's hold significant appeal for organisations to deliver growth and achieve dramatic savings in capital expenditures and operating costs by reducing complexity and increasing agility within their infrastructure.

There are many different hosting models to select when outsourcing the hosting and management of business functions. Consumers can choose models across a range where the security role is weighted more to the consumer (Infrastructure as a Service, Platform as a Service) or weighted more to the service provider (Software as a Service).

While the adoption of CSP's is driven largely by the need to reduce costs and

[1] Gartner Research, Cloud Application Infrastructure Technologies Need Seven Years to Mature, Mark Driver, December 2008.
[2] Ibid

leverage the capability and scale of a shared infrastructure, the implication from a security perspective is paramount. This is particularly relevant for highly regulated sectors where entities may utilise third parties for service delivery but must ensure that their engagement is consistent with mandated compliance requirements. For example:

- Australian Federal Government Agencies may adopt CSP's where they demonstrate value for money and adequate security (meeting the mandatory requirements outlined in Protective Security Policy Framework (PSPF)). Agencies will remain ultimately responsible for the information that is stored and/or processed in the cloud. Management must maintain assurance that the security of the cloud service provider is in accordance with the PSPF [3].
- All entities involved in the processing, transmission or storage of cardholder (credit card) data must comply with the Payment Card Industry Data Security Standard (PCI DSS) [4]. This includes managed service providers delivering services to maintain components such as routers, firewalls, applications, databases, physical security, and/or servers [5].

In a recent study conducted by the Ponemon Institute regarding security in the Cloud, the following findings are noteworthy [6];

The majority of CSP's:

- do not believe that their organisation views the security of their Cloud as a competitive advantage;
- do not believe that security is one of the most important responsibilities of the CSP;
- do not believe that their products or services substantially protect and secure the confidential or sensitive information of their customers;
- believe that it is the customer's responsibility to secure the Cloud;
- believe that CSP systems and application are not always evaluated for security threats prior to deployment;
- allocate 10% or less of operational resources to security and;
- do not have confidence that their customers' security requirements are being met.

It is useful to look back to the heritage of hosting services, because not everything about the cloud is new. When comparing cloud models to traditional hosting service delivery models it is noted that there are many differences in the approach. However, from a security perspective there are many similarities regarding the parameters that are needed to ensure a secure outcome from CSP's under any model adopted. In all models it becomes very difficult to address compliance (security) requirements where the responsibilities of the CSP have not been clearly defined and their role in delivering a compliant (secure) offering established.

[3] Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2011

[4] The PCI Data Security Standard (PCI DSS), provides an actionable framework for developing a robust payment card data security process - including prevention, detection and appropriate reaction to security incidents.

[5] PCI DSS Requirements and Security Assessment Procedures, Version 2.0

[6] Security of Cloud Computing Providers Study", Ponemon Institute (April 2011)

Benefits Presented by CSP

Key benefits offered by CSP's include [7]:

- Reduced capital costs – CSP's offers flexibility allowing enterprises the option of scalability without major financial obligations required for infrastructure purchase and maintenance. With the potential for minimal or negligible upfront expenditure, services offered or subscribed to are available on pay-per-use based on demand cycles. Additional cost savings are made by recapturing the lost value of underutilised infrastructure resources (hardware and software). This also presents an opportunity to experiment with new technologies and services without significant investment.
- On demand scaling – By providing unconfined capacity and increased flexibility, CSP's offer increased scalability for evolving IT needs. Service provisioning, in addition to scaling services up or down based on client demand are highly regarded features for the dynamic business.
- Faster time to market – CSP presents the ability to provision and utilise the services rapidly. This compares to traditional IT projects that may run well past their estimated project delivery time frame, including ordering, configuration and implementation. The net result fundamentality reduces complexity, costs and time delays, whilst increasing the agility of the business.
- Business innovation – A range of outsourced management options, rapid deployment and on-demand computing, allows businesses to focus on business development and innovation while capitalising on service delivery.
- Business resiliency – CSP accommodates business requirements for high availability and redundancy, thereby providing an opportunity to address potential service delay issues. Additionally, CSP's offer mirrored solutions that could be utilised in a disaster scenario, addressing requirements for a disaster recovery location. Generally, resiliency and capacity requirements are met by the CSP however, these should be carefully addressed by organisations prior to service provisioning.

Through selective engagement of the cloud model, CSP's can bring clear economic benefits, increased IT agility, real business impacts, and value across IT and business aspects of the organisation.

[7] The Economic Benefit of Cloud Computing
http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/

Key Risks and Challenges Presented by CSP's

As the CSP phenomenon gains momentum across the business spectrum, there is also an increasing trend of uptake of the CSP in highly regulated sectors that must comply with industry standards (PCI DSS, ISO 27000) [8] or government regulations (PSPF, ISM)[9] . CSP is transforming the way IT services are provided, consumed and managed.

Regardless of the industry an organisation operates in, the fundamental tenets of information security do not change. All organisations must be able to ensure the confidentiality, integrity and availability of information. The CSP must instil confidence and demonstrate its capability to deliver the desired business requirements as well as validate compliance with regulations/standards to third party auditors and business stakeholders.

As with the introduction of any new technology, it is important to be aware of the risks involved. With CSP's, the resultant risks are a convergence of several traditional risks in addition to the introduction of some unique challenges for organisations.

Specific risks related to CSP's include [10] ;

- Legislative and Regulatory requirements – Depending on the CSP model adopted, and due to the dynamic nature of the operations, it may not be known where the information actually resides. This may result in potentially conflicting domestic and international legal and regulatory requirements.
- Compliance Obligations – CSP's may not meet an organisation's compliance needs. In addition, not knowing the roles and responsibilities for compliance between the parties could result in non-compliance and penalties.
- Multi-tenancy – Systems hosted by CSP's are required to deliver high level services on demand which may not be practical to host from the organisation's private networks. Cloud offerings, and indeed many other hosting services, are built on virtualised platforms. As a result, there may be inadequate segregation between different customers (tenants) or regulated data that resides within CSP facilities.
- Data Security – Organisations can effectively enforce and monitor security policies when managing information on private networks (managed in-house). Enforcement of such security policies, however, becomes increasingly difficult for organisations that host their services at CSP's. This is particularly the case where security measures within the CSP facility are limited or lacking in visibility.
- Data Ownership – Managing data on behalf of an organisation requires acceptance of responsibilities for data handling. Business requirements for data availability and confidentiality must be addressed in the context of service level

[8] The ISO 27000 series of standards have been specifically reserved by ISO for information security matters, http://www.27000.org/index.htm

[9] Australian Government Protective Security Policy Framework, http://www.ag.gov.au/Protectivesecuritypolicyframework/Pages/default.aspx
The Defence Signals Directorate (DSD) produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT systems. It complements the Protective Security Policy Framework. http://www.dsd.gov.au/infosec/ism/index.htm

[10] Advancing public cloud computing: What to do now? Priorities for industry and government; Part two of the 2011 World Economic Forum project.

arrangements with the CSP. Failure to do so may result in the business facing penalties for breaches.

- Business Continuity Plans (BCP)/Disaster Recovery (DR) – Organisational requirements for BCP/DR must apply to outsourced environments as they do for in-house facilities. The recovery and continuity procedures of the CSP may not meet organisational requirements, resulting in possible financial loss and damage to reputation.
- Contractual agreements – Data may traverse or be stored in politically /economically unstable countries. The legal jurisdictions that may apply to the data can be a challenge to any organisation. Unclear rights and recourse for security breaches and incidents may have ramifications for liabilities. Contractual agreements should also clearly indicate exit clauses to stipulate not just the procedure for the organisation to terminate relationship with its CSP but more so what steps the CSP has to undertake removal of the organisation's data from its systems.

Mitigation Strategies

It is imperative that the risks organisations face when dealing with CSP's be managed effectively and on an ongoing and evolving basis from the start of engagement to when the services are provisioned and utilised. Directors have a duty of care to apply reasonable measures to protect sensitive client, business and employee data. Accordingly the selection of the CSP must be based on an assessment of their security capabilities, taking into account gaps in protection and compliance.

The Australian Federal Government has identified areas of weakness in contract and provided the following note in a recent paper: The contract between a vendor and their customer must address mitigations to governance and security risks, addressing who has access to the customer's data and the security measures used to protect that data. Vendor's responses to important security considerations must be captured in the Service Level Agreement or other contract. In some cases it may be impractical or impossible for a customer to personally verify whether the vendor is adhering to the contract, requiring the customer to rely on third party audits including certifications instead of putting blind faith in the vendor [11].

A good risk management and security program will address key controls to mitigate the business risks before measuring the potential benefit of using a CSP. Critical controls that organisations should evaluate are included below [12], but do not apply to every situation. That being said, understanding the controls and their limitations for organisations will assist in making the right trade-offs in order to design a strategy for risk mitigation.

Risk Management

In line with a risk management approach for in-house services, outsourced services should also be assessed against risk criteria. This is in order to identify critical assets, analysis of threats and vulnerabilities to those assets, in conjunction with developing an appropriate risk treatment plan. Lack of physical control of infrastructure renders a risk management process all the more important.

Traditional forms of risk assessment may not cover the requirements of CSP aspects such as a pay-as-you go model or multi-tenancy, and may therefore require new or modified procedures. An organisation's security framework or regulatory requirements may mandate, for example, vulnerability assessment, penetration testing and event log management. These may or may not be permitted by, or provided for by the CSP. As such, these factors must be addressed contractually.

Governance

As part of the organisation's security framework, security policies and procedures should be extended to accommodate the CSP. These should include defining baseline controls it is looking for in the context of its security policies and standards. Current governance practises followed by the CSP should be thoroughly assessed for adequacy, maturity and effectiveness for the scope of services offered. These

[11] Cloud Computing Considerations, DSD, April 2011
[12] CSA Cloud Security Alliance – Security Guidance for Critical Areas of Focus in Cloud Computing V 2.1

practices should support an organisation's business requirements and risk management needs during the design and development of service level agreements. The governance structure of the organisation and CSP should be included as criteria of the risk assessment process. The outcome of any assessment process, if acceptable, ought to be included in the service level agreements.

Regulatory compliance requirements form a critical element to any organisations security strategy. However, these requirements should not be the only driving factor, as regulations do not define in detail how to protect an organisation's information. Additionally, they do not address emerging threats and developments, such as mobile devices, social networking and privacy of personally identifiable information (PII). Accordingly, organisations should not focus on compliance requirements to get secure, but rather on protecting business information and effective implementation of security controls, including services provided by the CSP.

Third party

Organisations using CSP's which are themselves reliant on third-party services should conduct an end to end assessment on services including business continuity and disaster recovery, policies and procedures, backup facilities, procedures and incident management.

Disaster recovery planning must cater for scenarios for loss of the CSP's services and for the CSP's loss of third party services and their dependent capabilities. The CSP should be listed as the key contact point in recovery plans, together with defining roles and responsibilities for both the organisation and service provider.

Legal and Electronic Discovery

Duty of care must be addressed for contract term negotiation, post-contract monitoring, contract termination and transition of services to other service providers. The contract agreement should also address recovery and sanitisation of an organisation's data following the termination or transfer of contracts.

It is essential to ensure that the ownership of information hosted with the CSP always remains with the organisation (originator) and is retained in its original and authenticable format.

The locations of the CSP must be known to the organisation to ensure compliance with local laws that may have restriction on cross-border flow of data.

Compliance and Audit

Organisations should carefully analyse the impact of regulations on technology aspects, for example, infrastructure and applications, policies and procedures and data security. Using CSP's could present situations where organisational policies and procedures may require the ongoing implementation of potentially complex technical security controls mandated by regulatory requirements.

An organisation's compliance and audit requirements must be addressed at the engagement stage irrespective of where the information resides. It is therefore of the utmost importance to ensure service contracts are adequate to meet the organisations compliance and audit requirements prior to procuring CSP services.

Regulatory requirements change from time to time and it is also expected that the CSP's environment will be dynamic. As such, the organisation should ensure a "right

to audit" clause in the contract in order to ensure up to date regulatory requirements are being met. In certain situations the requirement can be addressed by security standard certifications (ISO 27001, PCI DSS). However, the scope of the certification should also be assessed to ensure it is applicable to the services being utilised by the organisation. It is reasonable to expect that the organisation initiating the audit pays for the audit. However, any remedial activity to address compliance or service delivery gaps should be for the CSP's account wherever it was their responsibility to deliver compliant services in the first instance.

Visibility in the Cloud

A successful CSP implementation will be one that is flexible enough to match an organisation's needs and expectations. Service level agreements could serve as the most effective tool for organisations to ensure that adequate protection of information is enshrined. In many cases, however, the CSP may not readily discuss security measures and controls because they consider them private.

Key questions organisations should consider when engaging with a CSP include;

- What services or information are you moving to the CSP? Is the service or information critical to business success?
- What is the impact on legislative, regulatory and compliance requirements by moving to a CSP? For example, Information Privacy Act, PCI DSS security standard.
- What are the implications on information ownership and usage rights when information resides on the CSP's premises?
- Does the CSP have adequate recovery and continuity procedures in the event of a loss of cloud services? Can this be guaranteed through Service Level Agreements?
- What types of technical and non-technical controls are implemented by the CSP to ensure data integrity and availability?
- What mechanisms are in place to ensure appropriate isolation from other tenants using the services? Segregation may be required at the network, operating system and application layers and most importantly there should be guaranteed isolation of the data that is stored (most likely on shared infrastructure).
- What provisions are made to ensure that change of the CSP or exit of contract does not incur additional costs and/or expose the organisation to additional risks? For example, and/or including, data retention risks?
- How are organisations able to restrict information from flowing through certain countries and legal jurisdictions? If not, what are the provisions made in the Service Level Agreements and contracts?
- How are the information security responsibilities for the organisation and CSP defined and addressed in the contracts?
- What are the reporting and monitoring mechanisms available to the organisation to ensure effective governance and management of the services migrated to the CSP?
- Does the organisation have the right to audit a CSP's effective implementation of security measures? If not, can the CSP give assurance by providing a recent report of an audit conducted by a reputable third party? If security issues or deviations are found, will the CSP remediate at their cost?
- What are the obligations and remedies between the parties? Are these addressed clearly in the contracts?
- Does the CSP have methods of notification for responding to data security breaches?

Conclusion

CSP's are actively developing and rebranding their services to capitalise on the rapid adoption of a plethora of outsourced managed hosting models. Such service offerings have grown exponentially and continue to gain traction because of the promised benefits these services present.

Many organisations are now selecting CSP's that offer infrastructure services. These companies are reaping the benefits of access to advanced technology at a fraction of the cost of making capital investments in dedicated systems.

Investment in shared technology services can deliver improved capabilities to multiple clients using shared services. Certainly CSP's and their offerings are here to stay. However, many organisations and users of these systems and services incorrectly assume that risks outsourced to the CSP are no longer their responsibility.

Whilst the use of CSP providers has become more prevalent due to the business benefits they bring, it is equally important to be mindful of, and evaluate, the risks they present. Put simply, if a business does not know its risks, it will not be able to determine the CSP which will best address their needs. Therefore strong governance and controls are an essential part of any decision to transition to a CSP. Additionally, governance and control activities must be managed throughout the information life cycle and should be reassessed regularly or in the event of a change. Organisations must engage people from legal, security and assurance disciplines to ensure the appropriate levels of security are achieved, whilst ensuring legislative obligations and regulations are met. It is critically important for an organisation to recognise that security drives compliance and not the other way around.

Unfortunately, the current information security programs of many organisation's do not adequately address the risks presented by the use of CSP providers, highlighting the fact that governance is needed more than ever to control and manage the risks. As such, organisations, when engaging with CSP's must demand the required level of assurance by asking appropriately tailored questions to make informed decisions around their risk appetite. As more organisations embrace such an approach, the market will increasingly recognise security as a differentiator for CSP providers.

About Sense of Security

Sense of Security Pty Ltd is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides you with a capability to assess your risk and deliver qualified guidance on how to protect your information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:

Web: www.senseofsecurity.com.au

Email: info@senseofsecurity.com.au

Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence