Cloud Computing Risks

By Richard Mosher – ISSA member, Kansas City, USA Chapter

Cloud computing risks still include data privacy, availability, service provisioning, malicious attack, and regulatory compliance. Mitigating the risks, now more than ever before, requires a mature vendor management program in which cloud service providers are tasked contractually with guaranteeing the information security requirements of their customers.

Abstract

The most recent development in information technology support for corporate business is the growing use of cloud computing. This trend presents a unique set of risks to corporate data that must be specifically addressed when considering this option. The issues involved are as old as information security. The risks still include data privacy, availability, service provisioning, malicious attack, and regulatory compliance. The venue has changed as technologies have morphed. Mitigating the risks, now more than ever before, requires a mature vendor management program in which cloud service providers are tasked contractually with guaranteeing the information security requirements of their customers.

Background

Cloud computing began years ago with the development of services such as online application offerings through application service providers (ASPs), infrastructure service providers such as Internet service providers (ISPs), and functional service providers such as managed security services providers (MSSPs). Following the development of virtual technology and other technological innovations, cloud computing services are now defined within three categories.

- **Infrastructure as a Service (IaaS)** – A computing infrastructure is delivered as a service, although the infrastructure, platforms, or applications within the environment may be managed and supported either internally or by the external entity.
- **Platform as a Service (PaaS)** – Computing platforms are delivered as a service; the infrastructure is managed by the service provider, but platforms or applications within the environment may be managed and supported either internally or by the external entity.
- **Software as a Service (SaaS)** – Computing applications are delivered as a service, and the infrastructure and platforms are managed by the service provider, but the application may be managed or supported either internally or by the external entity.

Of necessity, each of these involves the external management of particular functions by the external provider. For instance, an external IDS/IPS service generally involves an infrastructure, platform, and application managed by the service provider in providing the function. Likewise, the provisioning of HR services through an external application such as ADP must be supported by, and may be managed by, service provider personnel.

This picture is clouded to some extent because the industry recognizes that cloud environments may be external to the organization, entirely within the organization (private), or a hybrid (a mix of the two). An alternate option is a community cloud, which is an external cloud provided by a service provider designed and configured to support a specific type of application or data requirement, as in, for instance, a medical industry cloud designed to provide a HIPAA-compliant service. This discussion is focused exclusively on the risks involved in the use of clouds provided by providers external to the organization in either a pure external, community or hybrid cloud environment.

As is true for all outsourcing arrangements, external cloud computing services share a set of risks that are derived from the decision to permit corporate data to be processed by or reside upon devices outside of the corporate environment and under the control of an outside organization. Some of these risks are increased due to the inherent nature of cloud computing.

Data privacy risks

Access control

The decision to move corporate data and/or documents to an external cloud environment by its very nature requires that individuals within the service provider organization may have access to the data submitted to the cloud environment if service provider personnel need access to the data storage area in support of the service.[1]

To mitigate this risk, the organization can require that the service provider

- limit access to the data/files to essential personnel only;
- conduct background checks of those individuals to whom access will be granted;
- maintain proper records of approval, removal, and review of internal access to the data;
- monitor access to the data;
- train internal staff on requirements to protect the data; and
- if needed for compliance purposes, provide reports to the organization regarding access to the data records by support staff.

Internally, the organization can

- Contractually obligate the service provider to these requirements; and
- Monitor vendor compliance with the requirements.

Internal segmentation

Any cloud service provider is likely to support multiple organizations. If not properly structured and configured, the data architecture underlying the service could put the organization's data at risk of disclosure to other organizations.[2]

To mitigate this risk, the organization can require that the service provider

- implement internal barriers/segmentation between the data of different organizations; and
- conduct audits of data storage to confirm that the barriers are effective.

Once again, this requires that the organization contractually obligate and monitor vendor compliance.

Sub-contractors

Many cloud service providers themselves are composed of multiple layers of cloud services, with the originally contracted provider using other cloud providers to support their own services. The organization must therefore be prepared to enforce its needs within multiple layers of service providers through the originally contracted service provider. This issue is especially troublesome if the organization is under legal and/or regulatory compliance requirements. If this is the case, the organization is often held responsible for ensuring the compliance of its sub-contractors. The organization will therefore want to know the identities of sub-contractors in order to be able to track their compliance status. This can only be ensured through appropriate contract language.[3]

To mitigate this risk, the organization can

- if the organization is under an obligation to satisfy regulatory requirements, discuss this with the cloud vendor, and, if possible, require that the service provider provide the identities of all sub-contractors in order to confirm their compliance status;
- if this level of compliance monitoring is not required, request that the service provider agree contractually to enforce all identified requirements on its service providers as appropriate;
- require that the service provider implement a vendor management program to monitor the compliance of its vendors; and
- monitor the service provider's compliance with this requirement.

Data ownership

In the past it was not unusual for cloud service providers to claim ownership of all data/files submitted to their care, and to publicly state the right to redistribute all submitted documentation at will.[4]

To mitigate this risk, the organization can

- ensure that the service provider acknowledges the primacy of the organization's rights to the data submitted;
- contractually obligate the service provider to limit use of the data to that approved by the organization; and
- contractually require that the organization's data be returned and deleted upon severing the relationship.

1 Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*, March 2010, "Threat #3: Malicious Insiders," p. 10 – https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

2 Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," ACM, November 2009 – http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf.

3 Giles Hogben, "Perspectives on Cloud Security in the European Landscape," Cloud Security Delivery Imperatives 2011, ISACA Virtual Seminar, April 2011.

4 Carl Brooks, "Cloud SLAs the next bugbear for enterprise IT," TechTarget.com – http://searchcloudcomputing.techtarget.com/news/2240036361/Cloud-SLAs-the-next-bugbear-for-enterprise-IT?asrc=EM_EDA_14018952.

E-Discovery

Because the data/files submitted are now supported on systems belonging to an external entity (e.g., the cloud service provider), that data is now subject to discovery not only by legal actions targeting the organization, but may also be at risk of discovery and disclosure by legal actions targeting the service provider or any one of its other customers or service providers. The organization's data may therefore be compromised due to legal actions that may or may not directly involve the organization.[5] [6]

To mitigate this, the organization can

- ensure that the service provider is bound contractually to notify the organization of any required legal disclosure that may involve the organization's data; and
- make internal plans to address e-disclosure needs in such an event.

Data censorship

In some cases cloud providers retain to themselves the right to audit and censor any data submitted to the service. This can cause delays in the data posting process or changes to the data itself that may be unacceptable.[7]

To mitigate this risk, the organization can

- contractually define any such activities on the part of the service provider, and the process through which it is supported; and
- require the service provider to report any such activities to the organization.

Encryption

In the current state of the cloud processing industry, implementation of encryption for data "at rest" within the cloud remains relatively rare, or is expensive when available. It has been identified within some cloud services that are designed to meet specific regulatory requirements, but is not available within more common cloud services.

To mitigate this risk, the organization can:

- use cloud services only for those data services that do not require data encryption for data privacy purposes; or
- select a cloud service provider that can provide encryption if required;
- confirm that the service provider has implemented appropriate encryption controls;
- confirm that the service provider regularly tests those encryption controls; and
- ensure that appropriate key management practices are in place to support the encryption.

Availability risks

Service degradation

External services through a cloud provider involve connections over the Internet, any section of which is subject to congestion and outages on a periodic basis. In addition, the service may be degraded by a malicious attack, either due to the diversion of resources caused by an attack on the service provider, by the diversion of resources due to an attack upstream from the service provider (an attack on one of their service providers) and resulting congestion on the telecommunication lines, or by diversion of resources caused by a successful penetration and use of the service itself as the base for further attacks on other sites.

To mitigate this risk, the organization can

- use cloud services only for those applications for which degradation of service is not a significant issue; or
- obtain redundant lines to the service provider through alternate carriers that can provide alternate connecting lines to the service; and
- implement appropriate and feasible alternatives for services during periods of service degradation.

Service outage

Similarly, all service providers will, for one reason or another, incur service outages and performance issues on a periodic basis.

To mitigate this risk, the organization can

- confirm that the service provider has designed the service with adequate capacity and multiple service sources to limit outages;
- require a service level agreement with the provider with contractual penalties for less than acceptable availability performance levels;
- ensure that the defined level of availability is acceptable for business purposes;
- confirm that the service provider has an active backup program and recovery plan,
- confirm that the service provider recovery plan is tested regularly;
- determine if alternate service options are available for periods in which the service is not available; and
- implement appropriate and feasible alternatives for services during an outage.

5 Wendy Butler Curtis, Curtis Heckman, and Aaron Thorp, "Cloud Computing: eDiscovery Issues and Other Risk," *Orrick eDiscovery Alert*, June 28, 2010 – http://www.orrick.com/fileupload/2740.pdf.

6 Lucas Mearian, "How data security can vaporize in the cloud," *Computerworld*, October 15, 2009 – http://www.computerworld.com/s/article/9139404/How_data_security_can_vaporize_in_the_cloud_.

7 Joseph Granneman, "Data Protection and Access Control in the Cloud," *Security and Compliance in the Cloud*, ISACA Virtual Seminar, December 2010.

Service provisioning risks

Service changes

As all IT professionals know, technology firms come and go. Cloud service providers may fail, be acquired, or change their business models and discontinue a service at any time. As a result, the organization may lose access to its data or to the service upon short notice.

To mitigate this risk, the organization can

- contractually require a specified minimum period of notice for service changes;
- identify alternate service options that can be activated upon need; and
- maintain an updated internal copy of the data for emergency use.

Cost changes

As with any outside service, costs for cloud services will change over time. Such changes can make this type of service less cost effective, jeopardizing the purpose behind using the service in the first place.

To mitigate this, the organization can

- ensure that service costs and changes are defined in the service contract; and
- evaluate the cost/benefit/risk trade-offs of the relationship during each contract renewal.

Malicious activity risks

Likelihood of attack

Because cloud service providers support multiple businesses and must have their services available on the open Internet, they are at increased risk of being attacked through their website portals. After all, attackers tend to prefer target-rich environments, and cloud service providers concentrate multiple targets within their service areas. This situation is made worse by the fact that they must make web support and administration tools available to their customers as a part of the normal business model through the web portal, thereby leaving these tools accessible to attackers as well. As a result, the organization's data/files are at increased risk of compromise through an outside attack.[8]

To mitigate this risk, the organization can

- confirm that the service provider follows recommended security best practices in the development and coding of its web application, including code reviews and appropriate application security steps within each level of its infrastructure;
- confirm that the service provider performs vulnerability and penetration tests on a periodic basis and remediates any issues identified; and
- confirm that these practices have been audited and shown to be in place and operationally effective.

Regulatory compliance risks

Audit records

In many cases the systems supporting cloud services are managed by service provider personnel through their internal processes. Service providers, as is true for most organizations, usually decline to provide internal operational details to external customers. Obtaining auditable records for the systems can therefore be difficult. In addition, the audit tools available through individual service providers vary significantly. The tools available for this purpose must be evaluated for each service provider. Because verifying the functionality and controls of all supporting systems may be required for compliance with regulatory requirements, this becomes a significant risk.

Verifying the functionality and controls of all supporting systems may be required for compliance with regulatory requirements, becoming a significant risk.

To mitigate this risk, the organization can

- negotiate with service provider a mechanism through which supporting systems can be audited and verified, either through an audit performed by the organization's audit team or through a third party verification using SSAE 16 SOC 1 and SOC 3 reports, and include this in the contract;
- obtain copies of previous relevant service provider SAS 70/SSAE 16 reports or conduct regular audits of the provider; and
- ensure that appropriate audit reports are mandated contractually to meet the needs of the organization.

Storage location

Typically, the service provider may store all or part of the data/files on servers where it is convenient for them. This may include transferring the data to servers outside of the region or country of origin. Such a situation may or may not be permissible, based upon regulations under which the organization operates.[9]

8 Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*, March 2010, "Threat #1: Abuse and Nefarious Use of Cloud Computing," p. 8 – https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

9 Dr. Thomas Helbing, "How the New EU Rules on Data Export Affect Companies Running Cloud Computing and SaaS," cloudcomputing-vision.com, April 16, 2010 – http://cloudcomputing-vision.com/805/eu-rules-data-export-affect-companies-running-cloud-computing-saas/.

To mitigate this risk, the organization can require that the service provider

- assess the organization's legal and regulatory requirements, and determine if restrictions exist on whether it can permit its data to be stored outside of a specific legal jurisdiction;
- if the organization faces this type of restriction, include a discussion of this issue with any service providers considered as service providers;
- if possible, agree contractually to storage location restrictions that will keep the organization compliant with its regulatory needs; or
- if this is not possible, exclude the service provider from those to be considered for the service.

Lack of breach notice

In addition to all the other controls that are missing, the organization using cloud services also loses insight into and control over mandated breach notifications. More often than not, the organization may not even know that a breach has occurred until it appears in the evening news.[10]

To mitigate this risk, the organization can

- use cloud resources for only those data applications that do not have regulatory compliance requirements; or
- contract with a cloud service provider that is willing to assert contractually that they will notify the organization at once in the event of a possible breach.

Compliance

The issue of compliance validation for cloud computing applications is an open question. Little has been done in this area to date, and support for compliance requirements varies considerably between providers.[11]

To mitigate this risk, the organization can

- use cloud resources for only those data applications that do not have regulatory compliance requirements; or
- contract with a cloud service provider that is willing to assert contractually that they will maintain compliance with the regulation in question; and
- maintain a compliance verification program that validates the service provider's compliance with the requirements.

10 Ariel Silverstone, "Cloud Security: Danger (and Opportunity) Ahead," *CSO Online*, May 19, 2009 – http://www.cio.com/article/492999/Cloud_Security_Danger_and_Opportunity_Ahead.

11 "Cloud Computing: Benefits, risks and recommendations for information security," European Network and Information Security Agency (ENISA), November 2009 – http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

Mitigation summary

The use of external resources for cloud computing in its current state involves a number of risks. The key to proper mitigation of the risks in cloud computing is to determine appropriate controls for all relevant security provider operations just as if they were internal, and then to contractually obligate the service provider to comply with those controls. In the process of mitigating its risks, any organization making use of cloud computing resources should take a number of key steps.

1. Evaluate the risks involved in the use of cloud computing for a specific data application, and determine if the benefits to be gained offset the risks and the costs. This is especially critical if any regulatory compliance requirements are involved.
2. Assess the available cloud computing service providers to determine if any can provide the needed service while providing appropriate support in mitigating the identified risks.
3. Perform appropriate due diligence on the selected service provider to ensure their financial stability, and to confirm the promised support architecture is available.
4. Obtain copies of the service provider SAS 70 or the new SSAE 16 audit reports to confirm their controls, or perform an audit of the service provider to confirm these details.
5. Ensure that the service provider contract includes language specifying all required mitigating controls and reporting.
6. Implement a vendor management program to ensure ongoing compliance of the service provider with all necessary controls and service levels.
7. Ensure that all other appropriate internal mitigating strategies and options are implemented.

About the Author

Richard Mosher, CISSP, CBCP, CISA, CGEIT, QSA, is a professional consultant working in information security, risk management, regulatory compliance, business continuity, and IT audit as a staff member of Experis, a ManpowerGroup company. He has 25 years of experience in information security, is a former ISSA chapter president, former ISSA International board member, and an ISSA Distinguished Fellow, and is a periodic contributor to the ISSA Journal. He may be reached at Richard.mosher@experis.com.