Minimizing the Risks of Cloud Computing

January 2017

The Accelerating Trend of Cloud Computing

According to CIO Magazine, cloud computing has helped many enterprises transform themselves over the last five years, but experts agree that the market is entering something of a second wave, both for public cloud and private cloud services built and hosted in corporate data centers. The cloud market will accelerate faster in 2017 as enterprises seek to gain efficiencies as they scale their compute resources to better serve customers, says Forrester Research in a new report (Fall 2016).

"Enterprises with big budgets, data centers and complex applications are now looking at cloud as a viable place to run core business applications," says Forrester analyst Dave Bartoletti, primary author of the research. Forrester says the first wave of cloud computing was created by Amazon Web Services, which launched with a few simple compute and storage services in 2006. A decade later, AWS is operating at an $11 billion run rate.

Forrester found that 38 percent of 1,000-plus North American and European enterprise infrastructure technology decision-makers said that they are building private clouds, with 32 percent procuring public cloud services and the remainder planning to implement some form of cloud technology in the next 12 months. Also, 59 percent of respondents said they were adopting a hybrid cloud model.

The benefits of cloud computing are tremendous, but it is critical to manage and mitigate the associated risks of potential data loss and/or inaccessibility through proper foresight and procedures.

Risks Associated with Cloud Service Models

Below are three models that possess the characteristics of cloud computing as defined by The National Institute of Standards and Technology (NIST). Those characteristics include Broad Network Access, Rapid Elasticity, Measured Service, On-Demand Service and Resource Pooling. The chart depicts three Cloud Service Models and their associated components, which are color-coded to represent the responsibility that rests with the User versus the Provider. The bottom line is that, whether you or the cloud provider has responsibility, there are mitigating procedures within your control to ensure protection, access and mobility of data.

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Application Support and Data	Application Development , Support and Data	Application Support and data
Database Support	Database Support	Database Support
Virtualization	Virtualization	Virtualization
Operating System support	Operating System support	Operating System support

Key:

Component managed by User
Component managed by Provider

We will discuss each of the models, their advantages and risks or areas on which we encourage you to focus before entering into any contract with a cloud provider. Regardless of the model you choose, there are common risk areas:

- ***Contract terms and conditions*** – to ensure your data is secure and you have access by way of data security, data breach notification requirements, service level agreements and the timeframe to return your data and associated assets in the event you move to another cloud service provider.
- ***Security*** – to provide for data privacy and compliance with regulatory requirements such as the Health Insurance Portability, HIPAA, SOX, CJIS, PCI,ITAR, FIPS 140-02, Accountability Act and the Gramm Leach Bliley Act, as well as, meet state requirements for the protection of data. You must be aware of, and monitor, the processes and protective measures your provider uses to protect sensitive data and critical enterprise processes.
- ***Legal Compliance*** – working with your legal staff regarding state, national and international laws, specifically those around any data that is collected, stored and processed, especially around information being sent across borders to other countries.
- ***Audit rights*** **and reports** - to ensure proper controls and security of your information at the cloud service provider's data center locations. The SSAE 16 (soon to be SSAE 18) and SOC 2 reports are independent audits, which serve as a valuable resource to verify that the cloud service provider has the appropriate controls and related processes in place at the data center locations.
- ***Contingency plans*** – to quickly protect and mobilize your data in the event of disaster or the need to move your relationship or access your data under unfavorable conditions.
- ***Vendor Reputation/Track Record*** – review retention, get testimonials, and review customization offerings, uptime guarantees, partnerships and billing/charges.

We will start with the model that has the *least* number of areas under *User* control and thus, creates the most risk of losing access to data.

1. Software as a Service (SaaS)

Cloud-based applications—or software as a service—run on distant computers "in the cloud" that are owned and operated by others and that connect to users' computers via the internet and, usually, a web browser. Companies opt for this model when the desire is to not have to purchase, install, update and maintain software:

- Rapidly start using innovative business apps (e.g. Salesforce.com, payroll)
- Access apps and data from any connected computer
- Minimize lost data if computers break since data is in the cloud
- Scale the service to users' needs or elasticity

Areas for Consideration:

The key to mitigating risks starts with the contract you have with your provider, given the provider has 100% of the responsibility. There are often standard contracts (known as "click-wrap agreements") that tend to favor the provider.

Our suggestions include, but are not limited to:

- Develop an exit strategy even before you enter into a contract.
- Be aware that, in a SaaS model, there is normally a multi-tenant relationship (similar to an apartment house where tenants share common space), therefore your organization may find situations where you are unable to utilize several of your tools and processes (e.g., scanning tools) because they could adversely affect other "tenants".
- Redundant data centers across multiple locations will actually mitigate risk exposures associated with disaster recovery type events.
- Your provider's employees (database and systems administrators) have escalated permissions to the database and operating system, which can be used to access (or steal) your data or disrupt your critical applications. Determine whether the cloud service provider is maintaining the appropriate level of security (e.g., encryption) over your data at the two critical points - in transit and at rest. If the logical and physical security controls are not adequate, there is increased risk exposure of unauthorized access to your data.
- Obtain and review the SSAE 16, SOC 2 or similar type review completed of the cloud service provider to ensure data is adequately protected. If the cloud service provider does not have an independent review performed, determine if you have audit rights to have your own assessment performed.
- Implement an Information Security policy that defines the roles of your organization and the cloud service provider. The Information Security procedure should address processes that align with an off-premise technology support model where you most likely will not be able to use some of the tools that are traditionally used to maintain awareness.
- Understand how your data is protected in transit and at rest and whether encryption is being used to protect your data at all times.

2. Platform as a service (PaaS)

Platform as a service provides a cloud-based environment with everything required to support the complete lifecycle of building and delivering web-based (cloud) applications—without the cost and complexity of buying and managing the underlying hardware, software, provisioning, and hosting. Companies opt for this model when they want to deploy and migrate applications to both public and private clouds and want to:

- Develop applications and get to market faster
- Deploy new web applications to the cloud in minutes
- Reduce complexity with middleware as a service

In a PaaS cloud support model, the user does not manage or control the supporting cloud infrastructure, including network, servers, operating systems or storage. The User does have control over the deployed application and any application environments that are hosted. The PaaS cloud model allows the User the ability to focus on the deployment of applications without having to maintain the supporting infrastructure. As part of the application development, the consumer has the ability to add on security features.

Areas for Consideration:

- Use open and standard Application Program Interfaces (API's) as much as possible. Use of open and standard API's versus extensive customization (where there is heavy dependency on a specific cloud service provider), allows you to transition easier to another cloud service provider if necessary.
- Determine the security features necessary to be added at an application level.
- If the PaaS includes application storage, determine who is responsible for securing consumer data in storage and how it will be secured (e.g., client/application encryption, database encryption, proxy encryption).
- Determine the procedures and tools necessary to perform and maintain off-site data back-ups.
- Identify the tools for monitoring, logging and auditing.
- Ensure you receive an independent audit report (SOC 2) on the cloud service provider's security. The SOC 2 report is an independent audit of the cloud service provider to verify that required controls are in place. Processes should be in place to obtain and review the report annually.
- Understand the provider's data recovery processes and/or participate in the disaster recovery testing performed by the cloud service provider. Understand the redundancies provided by maintaining your applications at multiple data center locations.
- Understand the roles and responsibilities of the user and cloud service provider for Incident Management response.
- Determine whether the cloud service provider will allow you to perform vulnerability or penetration testing.
- Prepare a risk assessment to understand the various threats associated with operating in the cloud environment and what you would do to mitigate risks in the event your data or applications in the cloud are not available.

3. Infrastructure as a service (IaaS)

Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data center space on a pay-per-use basis. Companies opt for this model when they need to get up and running more quickly while cutting costs and want:

- Not to invest in its own hardware
- Infrastructure scales on demand to support dynamic workloads
- Flexible, innovative services available on demand

In an IaaS cloud model, the User's responsibility is the greatest, extending from the infrastructure to the application. Because you are responsible for the infrastructure (database and operating system) and the application, you have greater ability to deploy software and other practices that are similar to a traditional on-site technology support model. With an IaaS model, both your team and the cloud service provider will have access to system and database administrator type accounts and data, which makes your data vulnerable unless it is encrypted.

Areas for Consideration:

In an IaaS model you have the ability to define and manage security components of the cloud environment. You are managing the security in an off-premise model, therefore, the tools you deploy need to be effective in a virtual environment.

As part of the planning process, your team should:

- Define the network security and determine how web application firewalls and intrusion prevention software will be used for the inspection of inbound traffic to prevent malware or other threats from entering your cloud environment.
- Determine how data loss prevention software, database activity monitoring software, file integrity monitoring software and encryption will be used.
- Decide the type of authentication method that will be used and the placement of the authentication servers. We recommend that the servers that handle authentication be placed your on site to reduce the risk of the servers being compromised.
- Identify the tools to be used for scanning and maintaining continuous monitoring of the cloud environment.
- Identify the necessary Security Information and Event Manager (SIEM) tools to log activity and generate reports or alerts regarding suspicious or unusual activity
- Confirm and/or participate in the cloud service provider's disaster recovery testing exercise.
- Implement procedures to perform back-ups outside of what is offered by the cloud service provider.
- Ensure your cloud service provider maintains the appropriate level of security over your data at the two critical points - in transit and at rest. If the logical and physical security controls are not adequate, there is increased risk exposure of unauthorized access to your data. The greatest threat to your data are the provider's database and system administrators who have escalated permission. In an IaaS environment, the cloud service provider is responsible for the physical and environmental controls over the data centers. However, since you have responsibility for the application, database and some of the operating system support, clarify the roles and responsibilities for operating system support with the cloud service provider.
    - Implement an Information Security policy that defines the roles of your organization and the cloud service provider. The Information Security procedure should address processes that align with an off-premise technology support model.
    - The most effective way to understand the security at the data center used by the cloud service provider is to obtain and review the SSAE 16, SOC 2 or similar type review completed of the cloud service provider. Otherwise, determine whether you have audit rights to have your own assessment performed.

Conclusion

The cloud is a game changer when it comes to leveraging technology to support your organization, mange costs of equipment and software, ease of deploying new solutions and generate stronger performance, especially given the shortage of IT talent and cybersecurity threats. While the cloud models (Software as a Service, Infrastructure as a Service or Platform as a Service) move your data and critical applications off premise, the responsibility and ownership to understand the risk associated with operating in the cloud and to implement the appropriate processes and procedures to mitigate the risk still resides within your organization.

About SB & Company, LLC

SB & Company, LLC (SBC) is a leading minority-owned, full-service public accounting firm headquartered in Baltimore, MD with offices in Washington, DC, Philadelphia, PA, Gettysburg, PA, Richmond, VA and Hollywood, FLA. Founded in 2005, SBC's leadership leverage their backgrounds with the largest global accounting firms and a practical business approach to help clients make smart business decisions. We are committed to the highest quality of technical expertise and proactive client service in order to build lasting relationships and generate the value you deserve from a business partner. SBC is registered with the PCAOB.

For further discussion or if you have questions, please contact Rick Williams, our IT Risk Leader.

Rick Williams
IT Risk Principal
(410) 584-2218
rwilliams@sbandcompany.com