

Cloud Computing with Business Resiliency

Technology continues to mature to the extent where companies regardless of size may be able to utilize leading edge yet stable solutions and infrastructure. Storage, network, and computing systems have all increased in performance consistent with Moore's Law. Software solutions are now available to tie all these components together into a blended compute and storage infrastructure. It is called "Cloud Computing" leading this shift to an outsourced Information Technology ("IT"), possibly across the enterprise. This shift of computing based resources (internal to external) is a strategic initiative that needs to be seriously considered and has the ability to have direct impact on enhancing the technical recoverability and operational resilience of an enterprise. It may take some time before businesses are willing to move their core applications or their entire IT infrastructure to the cloud, but if they do, they need to know what the "Cloud" vendor's responsibilities are and what their own responsibilities and costs will be.

The intent of growing, managing and maintaining a business resilient enterprise is to ensure critical business data, systems, processes, human resources and infrastructure are up and running prior, during and post a business interruption event. Business resiliency is based upon two key operational initiatives:

- Disaster Recovery ("DR") for IT based systems
- Business Continuity ("BC") for business processes, human resources and infrastructure

An effective DR program will ensure the ongoing availability of core company data, IT systems and software. An effective BC program will ensure core business processes are connected; employees are knowledgeable of recovery efforts and procedures, vendor service agreements are in alignment with recovery needs, government controls are supported and the company premise remains viable. So, the multi-million dollar question is "what affect does cloud computing have on existing and future BC/DR programs"?

Cloud Computing and BC/DR

Every BC/DR program must take into consideration the business metrics that support a resilient enterprise. This includes the amount and type of risk associated with moving to an outsourced environment. There are some strong business reasons why companies outsource their IT departments to "the cloud". Below is a list of pros and con's as they relate to BC/DR and business requirements:

Pros:

1. Easy adoption for certain applications. Roadblocks to entry are small for certain web-enabled applications.

2. Human resources:
 - less internal technical support – reduction in FTE's
 - reduction in training requirements
 - reduction in overall facilities cost
3. Minimal or no Capital Expenditure (“CapEx”).
4. Redundant systems and infrastructure can exist within the cloud.
5. Scalability and flexibility to change services (assuming they're available).
6. Access to knowledge data. Only requirement is internet access.

Cons:

1. Difficult Adoption. Most legacy applications are not well suited to easily migrate to the cloud.
2. Company core data being managed by a third party.
3. Who has access to the company's core data may be unknown to the client.
4. Data security is dependent upon the vendor's security initiatives. These initiatives may not coincide with legal and/or governmental mandates stipulated by the client.
5. Type and level of redundancy within the cloud may not support the required business metrics.
6. Propensity to get locked into a single vendor.
7. Inconsistencies in global regulatory issues.
8. Less creativity and freedom to grow and/or change strategic business initiatives.
9. Leadership thinking the cloud solves everything for BC/DR – it doesn't.
10. Data replication with system redundancy may still be needed outside the cloud.

A key management and technology issue with any cloud computing environment is the continuous availability of the enterprises core data and information. The majority of cloud solution providers sell a High Availability (“HA”) solution with a single site focus. The HA offering supports real-time failover for the clients applications and servers that reside in a single site facility. Replication to a physically diverse HA site is not supported. When the primary site fails, core data and information become unavailable to/from the cloud. Therefore, an IT based DR strategy and plan is still needed to support continuous information availability.

The decision to sign up with cloud computing is a strategic initiative with ramifications across the enterprise. The business case to support a cloud computing environment may appear solid – it's a lease vs. buy analysis. However, moving the majority of an IT department off site to a third party vendor requires significant up-front due diligence while ensuring a business resilient

enterprise. Business Continuity requirements still exist across operations regardless of where the technology resides. Depending upon the vertical industry involved, the company may still be required to develop, support and defend both BC and DR plans. Assuming a cloud computing environment, some key topics of BC resiliency are:

1. Developing a BC plan that is in alignment with the new operating paradigm.
2. Validating data integrity through DR exercises and tests.
3. Validating BC processes through exercises and tests.
4. Training employees on recovery processes and tasks.
5. Training employees on emergency management procedures.
6. Perform BC exercises for work group recovery.
7. Pandemic planning is still a must.
8. Validation through external auditing may be required.
9. May desire to build a development and test environment outside the cloud thereby supporting internal data integrity and redundancy testing.

Business resilient objectives within a cloud computing operating environment do not go away - they just change the required recovery metrics and processes. However, from a technical perspective there are proactive opportunities to ensure the cloud environment supports data, system, infrastructure, and software redundancy. As with any business resilient model increasing redundancy across all operations increases the leased vs. buy cost model. Also, it's important that new Service Level Agreements ("SLA's") support the recovery capabilities demanded by the business. Each SLA should be exercised and tested within the DR and BC plans. As the new operating paradigm shifts to cloud computing the enterprises BC and DR plans change accordingly. There is no one size fits all solution and most companies will end up supporting a hybrid cloud computing model. Regardless of the operating environment, business resiliency should be on the front burner of every strategic initiative.

About the co-author

James M. Myers is the President & CEO of Contingency Now Inc. A professional risk management consulting company based in Los Angeles, CA. James can be reached at; 310-686-9094.