

# Cloud Computing: Issues and Strategies

---

By John C. Checco, CISSP CSSLP CCSK

On October 5 2010 the Wall Street Technology Association continued its technology education seminars in the Boston Financial District on the topic of “How to Securely Leverage Cloud Computing” with a keynote by Gartner Fellow David Cearley and supporting presentations by Cognizant, MetraTech, NetApp, Verizon Business and MGL. This article is a synopsis of this seminar. Many thanks to the following parties for permitting the selective redistribution of this material:

David Cearley (Gartner), Mike Seppi (MGL), Paul Roehrig (Cognizant), Shaun Mahoney (NetApp), Doug Zone (MetraTech), Mike Maffattone (Harvard Management Group), Madge Meyer (State Street Corporation) and the Wall Street Technology Association.

Rather than paraphrase each speaker’s presentation; it would be more useful to organize the review into four major sections that each speaker has touched upon:

- Cloud Concepts & Definitions
- Cloud ROI & Business Justification
- Cloud Migration Planning & Assessment
- Cloud-Specific Security Issues

## Everybody Sees a Different Cloud

There are many different definitions of a cloud, it all depends on perspective.

### Characteristics:

To reiterate some formal definitions:

**NIST:** Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Gartner:** Cloud computing is a style of computing where scalable and elastic IT-related capabilities are provided 'as a service' to customers using Internet technologies.

David Cearley notes that each definition is comprised of, or implies, five technical attributes:

- Resource Sharing,
- Service Based,
- Internet Technology,
- Scalable and Elastic, and

- Metered Usage.

### Perspectives:

Shaun Mahoney from NetApp delineated two broad perspectives of cloud, IT and Business Operations; and Mike Seppi from MGL extrapolated a third perspective of the cloud, then End-User.

- **IT:** focused on technical aspects; such as virtualization, managed provisioning, sharing resources or offloading workload.
- **Business Operations:** focuses on efficiencies; such as faster time to market, cheaper startup costs, more innovation, and moving capital costs to operational costs.
- **End-user – the consumer of cloud-based services:** focuses on the automation and abstraction of all the business processes; how it provides flexibility in their daily work, optimizes their workflow and allows them to be more productive.

*All three perspectives are correct.* Clouds can be all those things, but only if the organization approaches cloud computing with the appropriate mindset.

### Delivery Variations:

Gartner defines 5 major variations of cloud implementations, from the “Custom Private Cloud” to the “Shared Public Cloud” and several hybrid positions. Each delivery model varies by delineating which elements are hosted and managed by external providers who can access the services, and the degree and type of resource sharing across cloud consumers.

### Service Offerings:

Another aspect of cloud is the tier of cloud services, traditionally: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service).

Gartner identifies two additional emerging services in the cloud marketplace:

- Advanced Business Services (BPO)
- Information Services (Data Feeds, Analyses from disparate sources)

As more datasets get put into the cloud, there is an increased advantage (or liability) that these datasets will be used in an emerging class of aggregate business intelligence services – whether knowingly or not by the dataset owners.

### Justifying Cloud – What is the ROI?

*A decade ago, if someone approached me with the plan to take all my data and processes, host them dirt cheap in places where I cannot even pronounce, and have no control over the hardware/platforms they were running on and no idea of the legal ramifications of hosting in unknown locations... well, you get the idea. Brand it as “cloud” and suddenly my CTO is asking “why aren’t we doing this?”*

The largest differences though between then and now are:

- **The maturity of tools** and platforms actually delivers on the promise of scalability and security.

- **It's not about cost.** It's about all those important things we stated before: time to market, elasticity, offloading responsibility and innovation.

Of course, this brings up new issues: business complexities of offloading IT operations, and the legal aspects of data locality.

Shaun Mahoney states the business mindset of cloud computing: cloud is not about technology, but about organizational expectations.

Paul Roehrig from Cognizant concurs that the “cloud versus no cloud” debate is the wrong debate to have.

Every business should consider what, if any, data and processes can move to the cloud and its impact on the end-user (the consumer of such services). They may find that none of their existing business operations are good candidates, but to consider it for innovation and expanding new value propositions.

David Cearley notes that if an implementation's assets and usage are well-defined, predictable and consistent over time, then cloud infrastructure may not be a good fit. Cearley also makes the point that organizations pre-allocate physical assets and bandwidth resources based on only periods of peak usage – the fire department staffing model. Cloud deployment of these processes would gain immediate cost benefits from on-demand asset usage.

Mike Seppi also make the point that performance in the cloud can be increased through the use of intelligent parallelization techniques – but only where applications are built to take advantage of it.

Every IT department should be well-versed in the varieties of cloud implementations and delivery models. This allows them to work with their business counterparts to define and develop better value to the business. Remember, the business does not care HOW something is implemented, as long as it cost effective and can boost productivity or revenue.

Enterprise CIOs and CTOs: the business is your objective; the technologies are your tools. Do not justify projects based on “cloud” computing; base it on the business advantages that cloud provides.

For long-term ROI, Gartner sees the enterprises that develop cloud implementations that solve complex problems as eventually productizing/reselling these implementations – so cloud-service consumers can become cloud-service providers – providing additional revenue to the business. The best examples of this are Amazon (and of course Google). Who would think that Amazon, an online marketplace that started in book sales, would be a leader of cloud delivery platforms?

## **Preparing the Enterprise IT for Cloud Migration**

David Cearley outlines how management needs to approach cloud initiatives with the following aspects: Strategy, Governance, Security & Compliance, Development, Infrastructure & Operations.

Two main points in pre-planning a cloud migration:

- “You don't buy for the cloud; you build for the cloud,” David Cearley from Gartner.

- “Most successful organizational uses of cloud have a mix of cloud delivery models,” Mike Seppi from MGL.

So, what does this mean? It means that, like any other paradigm shift in business, it takes an enormous amount of assessment and planning.

Many companies offer assistance in infrastructure analysis (NetApp, MGL, Gartner, Cognizant, et al) and can walk enterprises through the assessment and planning processes.

First, let’s go back to basics; there are several key deficiencies in organizations regardless of cloud: Data Classification, Robust Access Control, Workflow Pipeline Visibility. Migrating to the cloud does not magically solve these issues; they need to be addressed well before any cloud assessment begins.

Assuming the above processes are properly defined, then the following assessment needs to take place:

- Workflow /Data Assessments:
  - Excess latent capacity, non-linear or unexpected usage, storage issues.
  - Framework applicability (re-work or abandon).
  - New value propositions, time to market.
  - Application Lifecycle Management – as in SDLC, plan appropriately for short-lived projects or long-term applications.
  - Information Lifecycle Management (ILM) – data is an intangible business asset, data is intellectual property; plan for ILM as if the business depended on it.
- Centralization and Virtualization of servers/applications/services.
- Correct cloud model for each implementation.
  - Be wary, though, “private customized cloud” is NOT simply virtualization.
- Prioritization and balance of application migrations and costs.

Every cloud delivery platform needs:

- Ample Resources
  - Doug Zone from MetraTech points out that different resources are used at different rates (CPU, memory, storage, and bandwidth).
- Resource Management
  - Automation of resource allocation and reclamation.
  - Ease of Use is important.
  - Resource Lifecycle Management – plan how long you’ll need the resource before committing to it.
- Service Management
  - Defining services, directories and catalogs in a standardized way.
- Access Management
  - Security, security, security.
  - David Cearley emphasizes, “Every cloud delivery platform needs a self-service portal that can be accessed to access a service as well as a defined API to access the service. If

you have to pick up the phone and call the vendor and ask them to set up or take down the service it is not a cloud service.”

- Usage Management
  - “Elasticity is finite,” Doug Zone from MetraTech.
  - To prevent over-extension of resources, a fair and robust charge-back systems needs to be in place; otherwise end-users will consume as many resources as are given them.
    - Goods Model – Allocation according to need; Marxist approach.
    - Services Model – Allocation based on ability to pay.
    - All the same underpinnings of the “Net Neutrality” argument.
- Metrics
  - Acceptability Criteria
  - Comparison against traditional development
- SLAs
  - Mike Seppi From MGL acknowledges that most cloud providers have customer service ratings well below par.
  - Also, service contracts for cloud providers can be vastly more complicated than just a hosting provider.
  - Flexible SLA choices. This can result in better cost allocation, but also can cause undue headaches. David Cearley explains, “Service levels and contracts are predefined and selected via the self-service portal and/or API. These service levels are incorporated into the automated operation of the standard service. It is not a cloud computing service if the SLAs that directly relate to the execution/operation of the service are defined only in a paper contract.”

Finally, there is the huge cultural change in migrating business solutions to the cloud.

- **Additional skill sets** are needed to analyze business workflow, architect solutions and design applications as it pertains to cloud computing. This is in addition to the existing analysts.
- **New IT responsibilities** responsible for managing all the different aspects of cloud operation.
- **Shifted IT responsibilities**, normally dedicated to issue tracking and implementations, also need to migrate to the new paradigm of support, development and deployment in the cloud.
- **Managing user expectations**, which were always difficult for IT departments, become even more complicated with the advent of implementations which:
  - Have aspects of operations out of IT’s direct control,
  - Target mobile devices,
  - Use disruptive technologies, and
  - Introduce new trials and tribulations with users.

## Security Issues for the Cloud

Security is an organizational issue, not a cloud issue.

Cloud security relies on extending existing policies, not creating new policies.

- Access
  - Role-Based Access Control
  - Federated Identity Management
- Resources
  - Data Classification
  - Resource Management
- Vendor Issues
  - Lock-in versus Portability
  - Taking advantage of vendor features
  - Lack of knowledge of internals
    - Data storage format
    - Application deployments
- Legal Aspects
  - Data Location Awareness
  - Operations Location Awareness
  - Delineation of Responsibilities
    - BC/DR planning, execution and costs
    - Log management, SIEM, breach notifications
  - Legal Obligations
    - Cloud provider legal obligations to organization subpoenas
    - Organization legal obligations to cloud provider subpoenas
  - Party Liabilities
    - Breaches
    - Intellectual Property litigation
  - Party Ownerships
    - Ex. Google owns your search data
  - E-Discovery
- Extending Existing Controls
  - SIEM packages
  - Cross-correlating incidents across distributed resources
- New Attack Vectors
  - Hypervisor
  - Internal networking
  - Shared resources
  - Cloud APIs (Management APIs as well as Operational APIs)

Michael Clark stresses that “Defense-In-Depth” is a necessity, but can be distributed between vendor and consumer. The important objective is to ensure there are no gaps in security.

Just like SLAs, security measures – threat landscape, attack vectors, risk valuations – need to be revisited routinely.

## **In a Nutshell...**

As David Cearley, Mike Seppi, Doug Zone and other presenters consistently emphasized: “Having no cloud strategy is no longer an option.”

Is your business ready to be: A consumer of public cloud services? An implementer of cloud platforms and infrastructure? A builder of cloud-capable solutions? All of the above? Or none of the above?

Every organization needs to have a cloud strategy. It is that *deep introspection of business operations* (albeit focused on cloud technologies), that benefits the organization – even if that final cloud strategy states that the no existing operations are ready for the cloud.

Know your cloud posture, know your business posture.

## **About the Author**

John C. Checco is Director at Iris Capital Partners, an M&A firm, where he specializes in due diligence of technology and information security. He is also founder of Checco Services, Inc., an information security consulting firm that markets the patented bioChec™ keystroke biometric technology. John currently holds CCSK, CISSP and CSSLP certifications, is a member of the Advisory & Content Committee of the WSTA, and is a secure member of Infragard NY Metro Chapter. He may be reached via email at [John.Checco@CheccoServices.com](mailto:John.Checco@CheccoServices.com).