The Cloud
inexpensive, rapid
deployment, ... and a governance issue?

a presentation for the
ISACA
Phoenix Chapter Meeting
Scottsdale, Arizona  14 May 2015
Hoyt L Kesterson II
Terra Verde
I AM NOT A LAWYER
I’ve looked at clouds...

- Before we discuss “the cloud” we should realize that it means different things to different people.
- As a business model it is revolutionary
  - for the consumer
  - for the road warrior
  - for the enterprise
- As a technology it seems to be a small jump from the distributed computing model.
From talking to a single computer...
To talking to a collection of them
From thin to thick and back again
To the Cloud

There’s a lot of advertising hype—products are now “in the cloud” without changing a thing.

Connecting from your laptop in the airport to your digital video recorder to watch a movie is a computer to computer connection, not a cloud operation (although the service may have been implemented as a cloud).

Using a remote third-party server does not put it in the cloud.
Here’s what NIST says

“a model for enabling ubiquitous, 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.”

NIST Special Publication 800-145
ISO/IEC WD closely aligned
The cloud—my explanation

*The cloud* is the result of the economies of scale made possible by the confluence of fast and inexpensive hardware, VM software that allows multiple instances of systems on a single instance of that hardware, ubiquitous and fast networks, and a relative maturity in the software that ties it all together.
Software as a Service (SaaS)—using a provider application running on the cloud infrastructure.

Platform as a Service (PaaS)—provides virtual platform with OS and below, e.g. network services. Client develops and tests applications.

Infrastructure as a Service (IaaS)—supplies and manages VM, storage, network services such as firewalls, infrastructure services such as time server. Client manages OS and above.
Virtual machines in the cloud

- Initially computers ran only one program.
- To run multiple programs concurrently, the OS fools each one into thinking they have access to the services and entire memory of the system—virtual memory.
- To run multiple systems, including the OS, the hypervisor fools each system into thinking it has exclusive access to the hardware hosting it—virtual machine.
Talking to the cloud

- The cloud can hold many types of services.
- Each type of service will have its own rules for talking to it—the protocol.
  - http and html for web browser to web server
  - smtp (+ things like s/mime) for email
  - ftp for file transfer
  - BitTorrent for peer-to-peer file sharing
  - Additional protocols may carry more commands such as shopping cart or SQL for database.
- Transmission is likely secured by TLS.
Examples of cloud services

IaaS—Amazon’s Elastic Compute Cloud (EC2), Microsoft Azure, IBM’s SoftLayer—Bluemix, big data services

PaaS—Elastic Beanstalk, Bluemix, .net, Ruby on Rails

SaaS—Google Apps, Salesforce, Adobe Creative Cloud, Zendesk, big data, e.g. Spark, Impala
...from both sides now

• For me, the technical guy, this is just evolution…
  – from a user connecting to a known computer…
  – to a user connecting to a service being performed in the enterprise environment, location unknown to the user but known to the IT staff…
  – to a user connecting to a service being performed in and outside the enterprise environment, location unknown to both the user and to the IT staff.

• IT can now focus on the security of its data and on service redundancy to provide continuity.
Changes for development

• Developers will use PaaS for application development.
  – Service provider supplies tools, framework, OS, storage, and infrastructure.
  – Application may be accessible from Internet.
  – Need stronger authentication to stop people from messing with your stuff, e.g. IP theft.
  – Ensure developer is not using sensitive data.

• Revise SDLC and policies.
Changes for testing

• IaaS can provide complex environment as needed for testing revised or new product.
• IaaS can be used to create a scaled-down facsimile of the enterprise environment.
  – Testing interactions between applications and between an application and services.
  – Testing business continuity and incident response plans
• Pick up after yourself—don’t leave sensitive data and IP behind
Changes for business

• In the 80's the IT organizations were slow to realize that groups within the enterprise were deploying their own low-cost information systems. PCs became ubiquitous.

• Chaos and pandemonium resulted.

• Using methods such as policy that chaos is just coming under control.
Whither governance?

• Just as IT is centralizing control over far-flung assets, along comes someone in the corporate badlands waving a credit card to deploy an application visible to, and accessible by, the world.

• It’s likely that system isn’t conforming to policy on data sensitivity, business continuity, or data retention.

• Destroying data while unaware of a…
Changes for lawyers

... a preservation order will irritate lawyers.

• Heaven help you—where is the original?
  – More of the turmoil caused by the increasing use of ESI (electronically stored information) complicated…
  …by not being sure of where that ESI is located.

• How do you request forensic investigation
  – into a shared environment?
  – into data being continuously replicated and moved?
  – into services that were rapidly deployed and then taken down when no longer needed?
Jurisdiction Issues

• Where is the data? The owner may not know.
  – A cloud provider may move data and virtual services continually to balance load, to provide redundancy, and to lower costs.
  – A cloud provider may subcontract server operation to a company located in countries with the cheapest taxes, labor, facility costs, and utilities.

• What if a company’s sensitive information is in a country with a lower bar for subpoenaing data?
Data protection issues

• Expect that the data will be encrypted.
• If the cloud service provider is encrypting the data, they have the keys.
  – The owner of the data doesn’t have final control as to who can see the data.
• The owner may choose to encrypt the data before moving it into the cloud.
  – This complicates the sharing of data.
• Keys get lost. They should be escrowed.
Process Protection Issues

• Processes executing in the cloud might have a hard time keeping secrets.
  – Those processes might have keys in the clear so they can decrypt data in the application.
  – If the storage service is encrypting or decrypting data, that data is in the clear for the process.

• The provider may have access to its customer’s encryption keys.
  – Will they resist turning that key over to other parties as rigorously as the data owner will?
Need to be PCI DSS compliant?

• If the provider isn’t PCI DSS compliant or if they will not grant access to your QSA
  – Be careful what card data you put in the cloud
  – If encrypted and the key is not accessible from the cloud, the cloud is out of scope

• Some providers have been certified compliant for the services they offer.

• Two important things in version 3 of DSS
Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.
Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.
Advice to in-house and external company counsel

• Evaluate your client’s contracts, e.g. service level agreement (SLA), with cloud providers.
  – Ensure that sensitive information is protected.
  – Ensure that the movement of very sensitive information is constrained, e.g. kept in the US.
  – Determine how the cloud service provider would respond to requests for access to company data.
  – What happens to data if contractual conditions are not met or the contract is terminated?

• Amend the preservation hold procedures to cover data kept in the cloud.
Chose wisely

- There is no capital T or C as of yet in the cloud.
- There is considerable opportunity for innovation and profit but also the potential for great exposure and risk.
- Just don’t listen to this guy.
Thank you. Questions?

Hoyt L Kesterson II  
Senior Security Architect  
Terra Verde  
Scottsdale, Arizona  
hoyt.kesterson@tvrms.com