Wrapping Audit Arms around the Cloud

Georgia 2013 Conference for College and University Auditors

Scott Woodison
Executive Director, Compliance and Enterprise Risk
Office of Internal Audit and Compliance
This presentation is based on work and a presentation developed by Phil Agcaoili and delivered to the Atlanta IAPP in February 2013 entitled:

**Cloud Assurance Basics**

**Phil Agcaoili**
CISO, Cox Communications
Founding Member, Cloud Security Alliance (CSA)
Co-Founder and Co-Author, CSA Cloud Controls Matrix (CCM)
Co-Founder Security, Trust, & Assurance Registry (STAR) and GRC Stack
agenda

• Intro to cloud computing
• Legal and privacy concerns to consider
• Latest developments of cloud security and assurance standards
Intro to cloud computing
What Is Cloud Computing?

• The “cloud” is a metaphor for the Internet
  – Leverages the connectivity of the Internet to optimize the utility of computing

• It is not new!
  – Search is a cloud application (Google, Yahoo, Altavista)
  – Internet-based email services are cloud applications (Gmail, Yahoo! Mail, Hotmail, AOL Mail)
  – Social networking sites are cloud applications (Facebook, MySpace, Forums)
  – Similar to time-sharing and service bureau services from the mainframe days, or ASP’s from the 90’s

• Accessible anywhere with Internet access
  – There are public, private, managed and hybrid clouds
The Consumer’s View of Cloud

...Everything is Cloud
Evolution Over The Years

- **1961**: John McCarthy proposed 'computer time-sharing technology' to be sold through utility business model (like electricity) in a lecture at MIT.
- **Mid 90's**: ASP (Application Service Provider) model with single tenant hosting of applications.
- **Early 00's**: Software as a Service (SaaS) model with multi-tenant hosting of applications.
- **Late 00's**: Cloud Computing with pay as you go model, leveraging virtualization for data center efficiencies and faster networks.
The Technical View of Cloud

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
## NIST Cloud Deployment Models

<table>
<thead>
<tr>
<th>Application (SaaS)</th>
<th>Applications at Scale (End users)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform as a Service</td>
<td>Execution Platforms at Scale (Developers)</td>
</tr>
<tr>
<td>Infrastructure as a Service</td>
<td>Infrastructure at Scale (System Administrators)</td>
</tr>
</tbody>
</table>

| Enabling Technology | Cloud Service Delivery at Scale (Public / Private Cloud Providers) |
Cloud Model :: Infrastructure as a Service (IaaS)
Cloud Model :: Platform as a Service (PaaS)
Cloud Model :: Software as a Service (SaaS)
### NIST Cloud Deployment Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Cloud</strong></td>
<td>Cloud infrastructure made available to the general public.</td>
</tr>
<tr>
<td><strong>Private Cloud</strong></td>
<td>Cloud infrastructure operated solely for an organization.</td>
</tr>
<tr>
<td><strong>Hybrid Cloud</strong></td>
<td>Cloud infrastructure composed of two or more clouds that interoperate or federate through technology</td>
</tr>
<tr>
<td><strong>Community Cloud</strong></td>
<td>Cloud infrastructure shared by several organizations and supporting a specific community</td>
</tr>
<tr>
<td><strong>Virtual Private Cloud</strong></td>
<td>Cloud services that simulate the private cloud experience in public cloud infrastructure</td>
</tr>
</tbody>
</table>

... and one other
Enterprise Deployment Models
Distinguishing Between Ownership and Control

**Internal Resources**
- All cloud resources owned by or dedicated to the enterprise

**External Resources**
- All cloud resources owned by providers; used by many customers

**Private Cloud**
- Cloud definition and governance controlled by the enterprise

**Public Cloud**
- Cloud definition and governance controlled by the provider

**Hybrid Cloud**
- Interoperability and portability among Public and/or Private Cloud systems
What This Means To Security

The lower down the stack the Cloud provider stops, the more security you are tactically responsible for implementing & managing yourself.

**Salesforce - SaaS**

**Google AppEngine - PaaS**

**Amazon EC2 - IaaS**
Legal and Privacy concerns to consider
Be Prepared for Change

• Cloud industry is immature and growing rapidly

• New players will rapidly emerge to fill new market niches

• Consolidation of the industry at some point is inevitable
  – You may not be as comfortable with new entity
    • Google, Amazon, IBM, Microsoft, Dell, HP, Cisco, CSC, and Verizon all active in this area
  – Big players will create standards for security and governance

• Cloud computing is disruptive to existing business models and IT practices
  – Disruptive technologies attract players who may not be around for the long term
Types of Issues

- **Location** (where is your data; what law governs?)
- **Operational** (including service levels and security)
- **Legislation/Regulatory** (including privacy)
- **Third-party** contractual limitations on use of cloud
- **Security**
- **Investigative/Litigation** (eDiscovery)
- **Risk allocation/risk mitigation/insurance**
Location Issues

• Where will your data be located?
  – The cloud may be the ultimate form of globalization

• What law governs?
  – You may or may not be able to control this by contract as the law in some countries can trump contractual provisions
  – State law is becoming increasingly relevant
  – Complying with a patchwork of federal and state privacy laws

• Storing data in certain regions may not be acceptable to your customers, especially the government
Operational Issues

• Vendor lock-in issues
  – Will you be bound to a certain application; platform; operating system?
  – Some critics, such as Richard Stallman, have called it “a trap aimed at forcing more people to buy into locked, proprietary systems that will cost them more and more over time”

• Can you transfer data and applications to and from the cloud?
Operational Issues

• Backup/data restoration

• Disaster recovery

• Acceptable service levels

• What do you do if the Internet crashes?
  – How is that risk allocated by contract?

• Data retention issues
  – There are many legal and tax reasons that a company must retain data longer than a cloud vendor is prepared to do so
Regulatory/Governance Issues

• The more of these issues you have, the slower you will move to cloud computing
  – Early growth in cloud computing will come from small and medium sized businesses and give them a competitive advantage
  – Portion of cost savings will have to be reinvested into increased scrutiny of security capabilities of cloud providers

• Some regions, such as the EU, have stringent rules concerning moving certain types of data across borders

• Cloud computing not regulated – “yet’
Regulatory/Governance Issues

- Patriot Act/UK Regulation of Investigatory Powers Act
- Stored Communications Act (part of ECPA)
- National Security Letters (may not even know of investigation)
- PCI (credit card information)
- HIPAA (health-related information)
- GLB (financial services industry)
- FTC and state privacy laws
- ITARS, EARS, other export or trade restrictions will impact where data can be stored and who can store it
- Video rental records
- Fair Credit Reporting Act
- Violence Against Women Act
- Cable company customer records
Contracts Will Be The Key Legal Enforcement Mechanism

• Privileged user access
  – Who has access to data and their backgrounds

• Regulatory compliance
  – Vendor must be willing to undergo audits and security certifications

• Data location
  – Can you control the physical location of your data?

• Security
  – Implementation is a technical matter; responsibility is a legal one
Key Contractual Issues

• Data segregation
  – Use of encryption to protect data—a sometimes tricky issue

• Recovery
  – What happens to your data and apps in the event of a disaster?
  – You should have test procedures in place

• Long-term viability
  – What happens to data and apps if company goes out of business?

• Investigative support
  – Will vendor investigate illegal or inappropriate activity?

• What happens in the event of a security breach?
Security Issues

• Physical security
  – Physical location of data centers; protection of data centers against disaster and intrusion

• Operational security
  – Who has access to facilities/applications/data?
  – Will you get a “private cloud” or a service delivered more on a “utility” model?

• Programmatic security
  – Software controls that limit vendor and other access to data and applications (firewalls; encryption; access and rights management)
  – Encryption accidents can make data unusable
Investigative/Litigation Issues

- Third party access
  - Subpoenas
    - You may not even know about them if vendor gets the subpoena
  - Criminal/national security investigations
  - Search warrants; possible seizures

- eDiscovery
  - How are document holds enforced; metadata protected; information searched for and retrieved?

- You must have clear understanding of what cloud provider will do in response to legal requests for information
Intellectual Property Issues

• The big issue is trade secret protection
  – If third parties have access to trade secret information, that could destroy the legal protection of trade secrets
  – This can be ameliorated by appropriate contractual non-disclosure provisions

• Same concern for attorney-client privileged information
Risk Allocation/Management

• No benchmarks today for service levels

• No cloud vendor can offer a 100% guarantee
  – The most trusted and reliable vendor can still fail
  – Should replicate data and application availability at multiple sites
  – Should you escrow data or application code?

• A premium will be charged based on the degree of accountability demanded

• Responsibility of customer to determine if it is comfortable with risk of putting service in the cloud

• Many publicly available cloud computing contracts limit liability of hosting provider to a level that is not in line with the potential risk

• Cloud computing contracts resemble typical software licenses, although potential risk is much higher
Insurance

• Will business interruption insurance provide coverage if your business goes down because of problem at cloud vendor?

• Do Commercial General Liability (CGL) or other types of liability coverage handle claims that arise from privacy breaches or other events at the cloud level?

• Are you covered if your cloud vendor gets hacked?
Checklist of Things to Consider

- Financial viability of cloud provider

- Plan for bankruptcy or unexpected termination of the relationship and orderly return of disposal of data/applications
  - Vendor will want right to dispose of your data if you don’t pay

- Contract should include agreement as to desired service level and ability to monitor it

- Negotiate restrictions on secondary uses of data and who at the vendor has access to sensitive data

- Understand cloud provider’s information security management systems
Checklist of Things to Consider

• Negotiate roles for response to eDiscovery requests

• Ensure that you have ability to audit on demand and regulatory and business needs require
  – Companies subject to information security standards such as ISO 27001, must pass to subs same obligation

• Make sure that cloud provider policies and processes for data retention and destruction are acceptable

• Provide for regular backup and recovery tests

• Consider data portability application lock-in concerns

• Understand roles and notification responsibilities in event of a breach
Checklist of Things to Consider

• Data encryption is very good for security, but potentially risky; make sure you understand it
  – Will you still be able to de-crypt data years later?

• Understand and negotiate where your data will be stored, what law controls and possible restrictions on cross-border transfers

• Third-party access issues

• Consider legal and practical liability for force majeure events
  – Must be part of disaster recovery and business continuity plan

• There is no substitute for careful due diligence
Latest developments in cloud security assurance

CSA Cloud Controls Matrix (CCM)
AICPA SOC Reports
CSA Open Certification Framework (OCF)
Research includes fundamental projects needed to define and implement trust within the future of information technology

- CSA continues to be aggressive in producing critical research, education and tools

- 22 Active Work Groups and 10 in the pipeline
GRC Stack

- Family of 4 research projects
- Cloud Controls Matrix (CCM)
- Consensus Assessments Initiative (CAI)
- Cloud Audit
- Cloud Trust Protocol (CTP)
Cloud Control Matrix

- Controls derived from guidance
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP, etc.
- Customer vs. Provider role
- Help bridge the “cloud gap” for IT & IT auditors
Consensus Assessments Initiative

- Research tools and processes to perform shared assessments of cloud providers
- Integrated with Controls Matrix
- Version 1 CAI Questionnaire released Oct 2010, approximately 140 provider questions to identify presence of security controls or practices
- Use to assess cloud providers today, procurement negotiation, contract inclusion, quantify SLAs
CSA STAR  
*(Security, Trust and Assurance Registry)*

- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties
Security Assurance - A Better Way
CSA Open Certification Framework (OCF)
OCF Level 1: CSA STAR Registry

- CSA STAR (Security, Trust and Assurance Registry)
- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire (CAIQ)
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties
- Available since October 2011
Questions & Answers

Thank you.

Scott Woodison
Scott.woodison@usg.com
Twitter @umichkid

404-962-3027