IT Cloud / Data Security - Vendor Risk Management Associated with Data Security

September 9, 2014

weaver
Assurance • Tax • Advisory
Speakers

Brian Thomas, CISA, CISSP
• In charge of Weaver’s IT Advisory Services, broad focus on IT risk, security and assurance issues

Reema Parappilly, CISA
• Manages advisory and attestation engagements, works in public and private sector
IT Advisory Services

Information Security
- Penetration testing
- Vulnerability assessment
- ISO 27001
- Data privacy

IT Audit
- IT internal audit
- External audit support
- SOX
- SOC reporting

IT Consulting
- Independent verification & validation
- IT assessments and planning
- Project risk management

Analytics
- Audit preparation
- Audit support
- Forensics support
- Management analytics
- Continuous monitoring
Weaver provides the information in this presentation for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, investment advice or professional consulting of any kind. The information included herein should not be used as a substitute for consultation with professional tax, accounting, legal or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided "as is," with no assurance or guarantee of completeness, accuracy or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose.
Contents

• Intro to the Cloud
• Cloud Risks
• Vendor Risk Management
• Third Party Assurance in the Cloud
• Current Trends
INtro to the cloud
Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet.

http://en.wikipedia.org/wiki/Cloud_computing
Intro to the Cloud

• Cloud computing not a new concept – John McCarthy, Stanford

• Wide scale adoption enabled by various factors

• Early examples
Business Benefits

• Scalability
• Focus resources on core competencies
• Reduced deployment time
• Right sizing capacity and demand
Basic Cloud Models

**SaaS** – Software as a Service
- Salesforce.com
- Hotmail.com

**PaaS** – Platform as a Service
- Microsoft Azure
- Google App Engine

**IaaS** – Infrastructure as a Service
- Rackspace
- Amazon Web Services
- SoftLayer
Cloud Models (cont.)

- Consumer can run applications in cloud
- Can access apps through various clients including browsers, mobile device etc

- Consumer gets an open platform/solution stack where he/she can deploy the application developed in language given by provider

- Consumer can provision computing resources (network, processing, storage etc) on-demand

- Software as Service (SaaS)
- Platform as Service (PaaS)
- Infrastructure as Service (IaaS)
Cloud Types

- **Private**: Used for a single organization; can be internally or externally hosted.
- **Community**: Shared by several organizations; typically externally hosted, but may be provisioned for open use for the public by a particular organization who also hosts the service.
- **Hybrid**: Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted.
- **Public**: Provisioned for open use for the public by a particular organization who also hosts the service.
Market Leaders - Managed Hosting

Magic Quadrant for Cloud-Enabled Managed Hosting, North America

14
# Public Cloud Adoption

## Top Public Clouds Used

<table>
<thead>
<tr>
<th>Place</th>
<th>Enterprise (1000+ employees)</th>
<th>SMB (Under 1000 employees)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>AWS</td>
<td>AWS</td>
</tr>
<tr>
<td>#2</td>
<td>VMware vCHS</td>
<td>Rackspace Public Cloud</td>
</tr>
<tr>
<td>#3</td>
<td>Azure PaaS</td>
<td>Google App Engine</td>
</tr>
<tr>
<td>#4</td>
<td>Azure IaaS</td>
<td>VMware vCHS</td>
</tr>
<tr>
<td>#5</td>
<td>Rackspace Public Cloud</td>
<td>Azure PaaS</td>
</tr>
<tr>
<td>#6</td>
<td>Google App Engine</td>
<td>Google IaaS</td>
</tr>
<tr>
<td>#7</td>
<td>SoftLayer/IBM</td>
<td>Azure IaaS</td>
</tr>
<tr>
<td>#8</td>
<td>Google IaaS</td>
<td>SoftLayer/IBM</td>
</tr>
<tr>
<td>#9</td>
<td>HP Cloud</td>
<td>HP Cloud</td>
</tr>
</tbody>
</table>

*Source: RightScale 2014 State of the Cloud Report*
CLOUD RISKS
Risk and the Cloud

- Depends on the type of cloud service being utilized
- Traditional IT risk areas apply to cloud computing:
  - Security
  - Processing Integrity
  - Availability
  - Confidentiality
  - Privacy
- Denial of service concerns
- Targets for breach
- Added emphasis on confidentiality / privacy

Picture Source: Bloomberg Businessweek
Unique Cloud Risks

Vulnerabilities with:

• Multi-tenancy
• Virtual exploits
• Ownership
• Need for backout plan
• Authentication to administrative panel / portal
Virtual Exploits

Hypervisors: The cloud's potential security Achilles heel

Summary: A cloud is only as secure as the hypervisors that support its virtual machines and how secure are those? That's a darn good question and one we tend to avoid looking at.

By Steven J. Vaughan-Nichols for Linux and Open Source | March 29, 2014 -- 01:25 GMT
(18:25 PDT)

Follow @sjvn

Get the ZDNet Cloud newsletter now

Ownership

- Basically, you own the data
- Grey area though – what about public cloud / free cloud?
- Geography considerations
- Penalty fees for backing out
Cloud storage provider Nirvanix is closing its doors

Two weeks' notice of service shutdown leaves customers scrambling to retrieve and move data to another cloud service

By David Marshall | InfoWorld

Cloud service provider Nirvanix may have inadvertently validated customers' fears centered around cloud storage. It was reported last week by U.K.-based website Information Age that Nirvanix has told its customers they have two weeks to find another home for their terabytes of data because the company was closing its doors and shutting down its service.

Founded in 2007, San Diego-based cloud storage provider Nirvanix, which targets enterprises with its public, hybrid, and private cloud storage services and usage-based pricing, had raised more than $70 million in venture capital funding, including a $25 million Series C round last May.
We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An *unauthorised* person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Reaching out to the address started a chain of events that revolved around the person trying to extort a large fee in order to resolve the DDOS.

Upon realisation that somebody had access to our control panel we started to investigate how access had been gained and what access that person had to the data in our systems, it became clear that so far *no* machine access had been achieved due to the intruder not having our Private Keys.

At this point we took action to take control back of our panel by changing passwords, however the intruder had prepared for this and had already created a number of backup logins to the panel and upon seeing us make the attempted recovery of the account he proceeded to randomly delete artifacts from the panel. We finally managed to get our panel access back but not before he had removed all EBS snapshots, S3 buckets, all AMI's, some EBS instances and several machine instances.
Code Spaces (cont.)

Code Spaces Status

Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of on-going credibility.

As such at this point in time we have no alternative but to cease trading and concentrate on supporting our affected customers in exporting any remaining data they have left with us.

All that we can say at this point is how sorry we are to both our customers and to the people who make a living at Code Spaces for the chain of events that lead us here.

In order to get any remaining data exported please email us at support[at]codespaces.com with your account url and we will endeavour to process the request as soon as possible.

On behalf of everyone at Code Spaces, please accept our sincere apologies for the inconvenience this has caused to you, and ask for your understanding during this time! We hope that one day we will be able to and reinstate the service and credibility that Code Spaces once had!
Regulatory Considerations

- US Regulations of note:
  - Cardholder information (PCI)
  - Protected Health Information (HIPAA / HITECH), Texas Medical Records Privacy Act
  - Breach notification (Red Flags Rule)
  - Publicly traded companies (SOX)
  - Personally identifiable information (GLBA)
  - Federal Information Security Management (FISMA)

- Transnational issues (EU, Japan, etc)

- Contractual responsibility vs. regulatory responsibility
Vendor Risk Management

• Have an overarching workflow with checklists to cover risk areas
  – Know where your data is
  – Know who the vendors are (including free tools!)

• Combine proactive activities with recurring initiatives
Key Personnel

• Involve the Key Players
  – Information Technology
  – Business Owner / Department Head
  – Procurement
  – Legal
Vendor Risk Management

• Define what can and cannot move to the cloud

• Define:
  – Minimum requirements
  – Must Haves
  – Exception Approval Process
  – Tiers
  – SLA
Vendor Risk Management

- Develop a policy and a process for identification and management
- Create a cloud inventory
  - Purpose
  - Owner
  - User(s)
  - Data Security Tier
  - Availability Tier
- Corporate Applications
  - ERP System
  - Payroll
  - SOX Systems
  - PCI - tokenization
- Personal Applications
  - Drop Box
  - Mobile BYOD
- Paid & Freeware
Assessing Vendors

- Financials
  - Reputable
  - Viable
- System Functionality
  - Implementation / Transition
  - Interface Management
- Availability Needs
- Security Considerations
Assessing Vendors - Security Considerations

- Authentication
- Account Lockout
- Administration
- Data Ownership
- Subcontractors’ Access

- Data Integrity Monitoring
- Portability
- Logging
- Security Measures
- Breaches & Notifications
Managing Vendors - Recurring Initiatives

- Periodic Status Meetings
- Review Cloud Inventory
- Review Access
- Client Audit
- Third Party Assurance
THIRD PARTY ASSURANCE
Audit Considerations

- Right to audit clause in contract
- Understanding of how the service is provided to you and the risks thereof
- Knowing where your data is
- Leverage existing third party assurance
Assurance in the Cloud

- AICPA SOC Reporting
- ISO 27001
- CSA CCM
- HITRUST CSF
- PCI DSS ROC
- FedRAMP: NIST 800-53
<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th><strong>Primary Use</strong></th>
<th><strong>Driver</strong></th>
<th><strong>Provider</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 1</td>
<td>Internal controls over financial reporting</td>
<td>Sarbanes-Oxley, FDICIA, MAR</td>
<td>CPA firms</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Other operational controls</td>
<td>Various regs (SOX, HIPAA, GLBA, TMRPA, Dodd-Frank, etc.); Contractual / SLA</td>
<td>CPA firms</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>Information security</td>
<td>Marketing; Europeans</td>
<td>ACBs</td>
</tr>
<tr>
<td>CSA CCM</td>
<td>General assurance to customers about soundness of security</td>
<td>Marketing</td>
<td>ISO 27001 firms, CPA firms (SOC Report)</td>
</tr>
<tr>
<td>HITRUST</td>
<td>Security of PHI, covered entities managing business associates</td>
<td>HIPAA</td>
<td>HITRUST firms</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Merchants, service providers</td>
<td>Credit card fraud / identity theft</td>
<td>PCI firms</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal government</td>
<td>Cyber security</td>
<td>Accredited 3PAOs</td>
</tr>
</tbody>
</table>
SOC Resources

SOC Reports, Logos, FAQs, Brochure & Peer Review Requirements

- SOC 1
- SOC 2
- SOC 3
- SOC Logos
- SOC FAQs: Technical Practice Aids TIS Section 9520 and TIS Section 9530
- SOC Brochure
- SOC Privacy Resource
- SOC Toolkit for Firms
- SOC Toolkit for Service Organizations
- Peer Review Requirement

### CCMv3 Cloud Controls Matrix Version 3.0

#### Control Domains

<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM v3.0 Control ID</th>
<th>Control Specification</th>
<th>Architectural Relevance</th>
<th>Corp Gov Relevance</th>
<th>Cloud Service Delivery Model Applicability</th>
<th>Supplier Relationship</th>
<th>Scope Applicability</th>
<th>AICPA TS Map</th>
<th>AICPA Trust Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity &amp; Access Management</td>
<td>IAM-13</td>
<td>Utilizes programs capable of potentially auditing system, object, network, virtual machine, and application controls shall be restricted.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>K</td>
<td>K</td>
<td>K</td>
</tr>
<tr>
<td>Infrastructure &amp; Virtualization Security</td>
<td>IWS-01</td>
<td>Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or integrity anomalies, and to support forensic investigation capabilities in the event of a security breach.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Infrastructure &amp; Virtualization Security</td>
<td>IWS-02</td>
<td>The provider shall ensure the integrity of all virtual machine images at all times. Any change made to virtual machine images must be logged and an alert issued regardless of their running state (i.e., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customer through electronic methods (e.g., portable media).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Infrastructure &amp; Virtualization Security</td>
<td>IWS-03</td>
<td>An industry- and mutually agreed-upon external time source shall be used to synchronize the systems clocks of all relevant information processing systems to facilitate tracking and reconstitution of activity timelines.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Infrastructure &amp; Virtualization Security</td>
<td>IWS-04</td>
<td>The availability, quality, and adequate capacity and resources for information systems processing and processing recovery must be explicitly defined, documented, and managed.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

[https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/](https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/)
CURRENT TRENDS
AWS Compliance

AWS Compliance enables our customers to understand the robust controls in place at AWS to maintain security and data protection. Because you’re building systems on top of the AWS cloud infrastructure, the compliance responsibilities will be shared. AWS Compliance provides assurance related to the underlying infrastructure and your organization owns the compliance initiatives related to anything placed on the AWS infrastructure. The information provided by AWS Compliance helps you to understand our compliance posture and to assess your organization’s compliance with your industry and/or government requirements.

AWS Assurance Programs

The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including:

- HIPAA
- SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
- SOC 2
- SOC 3
- PCI DSS Level 1
- ISO 27001
- FedRAMP(SM)
- DIACAP and FISMA
- ITAR
- FIPS 140-2
- CSA
- MPAA
Cloud Service Providers Fight Back, Challenge NSA

Facing a real business threat from the fallout from the NSA’s intelligence gathering, tech sector luminaries are expanding their presence in Washington as they lobby for surveillance reforms.

By Kenneth Corbin  
Wed, February 26, 2014

CIO — For U.S. cloud computing companies that have long been fighting to defend the privacy protections involving data stored in their servers or passing over their networks, the ongoing revelations about the extent of the NSA’s surveillance activities could carry a huge price tag.

For years, in markets such as Western Europe, cloud providers like Google and Microsoft have been trying to beat back concerns voiced by would-be customers — and stoked by competitors and governments — that the Patriot Act and other laws render data stored with American firms readily accessible to the U.S. government.

But the protectionist policies that some countries were pursuing — restricting cross-border data moves — are now being revisited as companies look to gain traction in Europe and elsewhere.

Most Recent Government Stories

- Microsoft’s General Counsel Calls on Congress to do More to Protect Users’ Private Data
- Hadoop Analysis Now Tackling IoT to Improve Transit
- NASA to Launch Asteroid-Grabbing Spacecraft in 2019
- House Approves Effort to Limit NSA Searches of US Data

Cisco buys Assemblage to keep pushing modern collaboration

The great tech lull of 2014

The two most important things at Google I/O
## Concerns re. Cloud

### Top 5 Challenges Change with Cloud Maturity

<table>
<thead>
<tr>
<th>Place</th>
<th>Cloud Beginners</th>
<th>Cloud Focused</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Security (31%)</td>
<td>Compliance (18%)</td>
</tr>
<tr>
<td>#2</td>
<td>Compliance (30%)</td>
<td>Cost (17%)</td>
</tr>
<tr>
<td>#3</td>
<td>Managing multiple cloud services (28%)</td>
<td>Performance (15%)</td>
</tr>
<tr>
<td>#4</td>
<td>Integration to internal systems (28%)</td>
<td>Managing multiple cloud services (13%)</td>
</tr>
<tr>
<td>#5</td>
<td>Governance/Control (26%)</td>
<td>Security (13%)</td>
</tr>
</tbody>
</table>

*Source: RightScale 2014 State of the Cloud Report*
Concerns re. Cloud

CSA

TOP DOWNLOADS

<table>
<thead>
<tr>
<th>TITLE, DESCRIPTION</th>
<th>VERSION</th>
<th>RELEASE DATE</th>
<th>DOWNLOAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Guidance</td>
<td>3</td>
<td>11/14/2011</td>
<td>Download</td>
</tr>
<tr>
<td>Cloud Controls Matrix</td>
<td>3</td>
<td>09/26/2013</td>
<td>Download</td>
</tr>
<tr>
<td>Consensus Assessments Initiative Questionnaire</td>
<td>1.1</td>
<td>09/01/2011</td>
<td>Download</td>
</tr>
<tr>
<td>The Notorious Nine: Cloud Computing Top Threats in 2013</td>
<td>1.0</td>
<td>02/25/2013</td>
<td>Download</td>
</tr>
<tr>
<td>Privacy Level Agreement (PLA) Outline for the Sale of Cloud Services in the European Union</td>
<td>1.0</td>
<td>02/25/13</td>
<td>Download</td>
</tr>
</tbody>
</table>

https://cloudsecurityalliance.org/
Current Cloud Trends

1) Personal cloud challenges for IT departments
2) IT as a service broker
3) Cloud client architecture
Takeaways
**Contact Information**

**Brian Thomas**  
713.800.1050  
brian.thomas@weaver.com

**Reema Parappilly**  
832.320.3254  
reema.p@weaver.com