Dispelling the Myths about Cloud Computing Security

security is no longer an hinderance to the cloud!

Leo F. Howell, CISSP CISA CCSK
Knowledge MYTH
we are all talking about the same cloud

Discussion
cloud computing architectural framework
NIST Model for Cloud Computing

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Public
Private
Hybrid
Community
CSA Cloud Reference Model (SPI)

- Presentation Modality
- Presentation Platform
- APIs
- Application
- Data
- Metadata
- Content
- Integration & Middleware
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities

Source: Cloud Security Alliance
## Cloud Service Model Example

<table>
<thead>
<tr>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services</td>
<td>Box</td>
<td>Dropbox</td>
</tr>
<tr>
<td>EC2</td>
<td>Rackspace</td>
<td>CrashPlanPro</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Azure</td>
<td></td>
<td>Fedora OpenShift</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AppFog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WordPress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intuit QuickBase</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Salesforce</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Google Apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Office 365</td>
</tr>
</tbody>
</table>
Jericho Cloud Cube Model

source: www.jerichoforum.org
Knowledge MYTH

the cloud is crystal clear to all of us!

DEBUNKED
Responsibility MYTH

the CSP takes care of security

Discussion

security responsibilities in IaaS, PaaS, SaaS
IaaS Security Responsibilities

- Build secure systems & segregate by classification

**APIs**

**Management Plane Security**
- OS Hardening
- Patching
- Host-based Firewall
- Network Firewall
- Antivirus
- Crypto-key Management

**Host IDS**

**API Security**
- Hypervisor Virtual Firewalls
- Software Defined Networking

**MULTI-TENANCY SECURITY**
- SAN Encryption

**Infrastructure as a Service (IaaS)**
- Secure
- SAN
- Storage

**Core Connectivity & Delivery**
- Abstraction

**Hardware**

**Facilities**
- Datacenters
PaaS Security Responsibilities

- Secure Development
  - SDLC security
  - Threat modeling
  - Masking, Tokenization
  - Static & dynamic analysis
  - Fuzzing
  - App-level encryption

- Secure Deployment
  - Code review
  - V-scanning
  - Pen-test

- Secure Operation
  - SSL access
  - Id & Access
  - V-scans
  - Pen-tests
  - Monitoring

Integration & Middleware

strong emphasis on application security

Infrastructure

Infrastructure Security

Consumer...
SaaS Security Responsibilities

- **Presentation Modality**
- **Presentation Platform**
- **APIs**
- **Application**
- **Data**
- **Metadata**
- **Content**

---

- **Software as a Service (SaaS)**
  - **Integration & Middleware**
  - **APIs**
  - **Core Connectivity & Delivery**
  - **Abstraction**
  - **Hardware**
  - **Facilities**

---

- **SecDev, SecDep, some SecOps**

---

- **Basic SecDep and some SecOps**
- **Identity & Access Management** (perimeterized or deperimeterized)
- **Grouping & Role-based Access CTRL**
- **Basic application logic & form-based CTRLs**
- **Special attention to BCP/DR due to lock-in risks**
- **Data Protection primarily handed off to CSP, so need strong RFP/Contract**

---

- **CSP...**

---

- **Consumer...**

---

- **Infrastructure and Platform Security**
Security Impact by Cloud Architecture

The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.

Source: Cloud security Alliance
Responsibility MYTH

consumers are mostly responsible for security in IaaS, then PaaS, then SaaS

DEBUNKED
Geo-Location MYTH
you can’t control where in the world your data is stored

Discussion
security considerations for international data storage and processing
Geo-Location Control over Cloud Data

• Offshore storage is a key consideration when selecting a CSP

• Laws and regulations (e.g., ITAR/export controls, DFARS, certain PII or PHI) may prevent offshore storage of data

• CSPs are beginning to address this - e.g., you can configure GoogleCloud to prevent offshore storage

• Don’t just focus on storage. What about geo-location for processing?

• Some cloud vendors provide the option for domestic storage only - just pick the right one!
Geo-Location MYTH
you can determine where your data is stored, just pick the right CSP and contract it in
Confidentiality MYTH

_CSPs and their sub-contractors have unfettered access to your data_

Discussion

encryption and key management in the cloud
Data Confidentiality in the Cloud

• **Tokenization** - replace sensitive data elements with tokens

• **Masking** - hide sensitive data with replacement characters before clouding

• **Encryption** without key management is useless

• **Crypto-shredding** - encrypt the data and throw away all copies of the key to securely delete
Confidentiality MYTH

encrypt your data and control the key

DEBUNKED
Incidents Response MYTH

*IR can’t be done in the cloud*

Discussion
incidents response and forensics in the cloud
What can you do as a Consumer in IR?

- **Prepare**
  - Contacts
  - Roles and responsibilities

- **Detect & Analyze**
  - Least capabilities in SaaS
  - Some capabilities in PaaS
  - Most capabilities in IaaS

- **Contain, Eradicate, Recover**
  - Shut down access to SaaS, no logs
  - Adjust app controls in PaaS, maybe application logs available
  - Take snapshot in IaaS, shut down servers, firewall blocks, review non-network logs

- **Post-incident Activities**
  - Similar to traditional

Remember! **Consumers have the highest level of controls in IaaS and the least control in SaaS - same is true for visibility in the incident management lifecycle.**
Incidents Response MYTH

*IaaS provides the most capabilities for IR; SaaS provides the least*

*DEBUNKED*
Assurance MYTH

the is no way to measure security in the cloud and provide assurance

Discussion

auditing and measuring security in the cloud
Measuring Security in the Cloud

- Service Organization Controls
  - SOC 2/SOC 3 - confidentiality, integrity, availability at the CSP
  - Type 2 SOCs test effectiveness and shows the auditor’s results

- PCI compliant clouds; HIPAA compliant clouds

- FedRamp compliant GovCloud

- Cloud Controls Matrix (**CCMv 3.0**)

- Create your own checklists
Assurance MYTH
measuring standards are emerging, you just need to know what to ask for
DR/BCP MYTH
you don’t need a DR/BCP plan for cloud services

Discussion
DR/BCP for cloud services in the cloud
Disaster Recovery and BCP in the Cloud

• More resilience in the cloud

• Avoid over reliance on a single provider; avoid vendor lock-ins

• Have you planned for the disaster of the vendor suddenly going out of business?

• DR responsibilities shifts but DR planning is still necessary, especially in a SaaS cloud
DR/BCP MYTH

the cloud may be resilient but you still need to plan, including for failed CSPs

CONFIRMED
Conclusion

Security can no longer be seen as an hinderance to moving to the cloud

But, tread lightly and diligently!
Contact
Leo F. Howell
Assistant Director, IT Policy and Compliance
NC State University
lfhowell@ncsu.edu

Resources:
Cloud Security Alliance (CSA)
www.cloudsecurityalliance.org
Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing
https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

CCMv3.0 Download:
https://cloudsecurityalliance.org/research/ccm/

The Jericho Forum:
www.jerichoforum.org