The Top 3 Risks of Moving to Cloud

Andrew Hay, CTO, LEO Cyber Security
+1.415.940.9660
andrew.hay@leocybersecurity.com
https://www.leocybersecurity.com
@andrewsmhay

2018 SANS Cloud Security Summit & Training
• Co-Founder and Chief Technology Officer (CTO) @ LEO Cyber Security

• Former:
  • CISO @ DataGravity
  • Director of Research @ OpenDNS
  • Chief Evangelist & Director of Research @ CloudPassage
  • Senior Security (Industry) Analyst @ 451 Research
  • Information Security Officer in higher education and financial services

• Blogger, author, and rugby coach
Introduction

• There are many security challenges/differences in cloud computing
• Some are more technical and some are more “macro” level issues
• Given the amount of time we have today, we’re going to focus on the top 3 risks of cloud computing as they relate to Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)
  • Security Controls in (and not in) the Cloud
  • Data Security and Traceability
  • Regulatory Compliance and Governance
The 3 Big Players In Cloud Hosting

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform
# Responsibility Zones

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance &amp; rights management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client endpoints</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; directory infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Always retained by customer**:
- **Varies by Service Type**: Transfers to Cloud Provider
Security Controls In (and not in) The Cloud

On Prem

Host-based controls (FW, HIDS, AV, etc.)

PaaS

PaaS

Host-based controls (FW, HIDS, AV, etc.)

IaaS

Host-based controls (FW, HIDS, AV, etc.)
Security Controls In (and not in) The Cloud

**On Prem**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)

**PaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)

**IaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
On Prem Security Controls In (and not in) The Cloud

- **Host-based controls (FW, HIDS, AV, etc.)**
- **Network-based controls (FW, IDS, etc.)**
- **Web application security**

**PaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security

**IaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security

- Only via software
Security Controls In (and not in) The Cloud

**On Prem**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security
- Encryption at rest (local storage & DB)

**PaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security

**IaaS**
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security

- Encryption at rest (local storage & DB)

- Only via software
Security Controls In (and not in) The Cloud

On Prem
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security
- Encryption at rest (local storage & DB)
- OS and application hardening

PaaS
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security
- Encryption at rest (local storage & DB)
- Some control

IaaS
- Host-based controls (FW, HIDS, AV, etc.)
- Network-based controls (FW, IDS, etc.)
- Web application security
- Encryption at rest (local storage & DB)
- OS and application hardening
Security Controls In (and not in) The Cloud

<table>
<thead>
<tr>
<th>On Prem</th>
<th>PaaS</th>
<th>IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="host-based-controls.png" alt="icon" /> Host-based controls (FW, HIDS, AV, etc.)</td>
<td><img src="network-based-controls.png" alt="icon" /> Network-based controls (FW, IDS, etc.)</td>
<td><img src="host-based-controls.png" alt="icon" /> Host-based controls (FW, HIDS, AV, etc.)</td>
</tr>
<tr>
<td><img src="network-based-controls.png" alt="icon" /> Network-based controls (FW, IDS, etc.)</td>
<td><img src="web-application-security.png" alt="icon" /> Web application security</td>
<td><img src="network-based-controls.png" alt="icon" /> Network-based controls (FW, IDS, etc.)</td>
</tr>
<tr>
<td><img src="encryption-at-rest.png" alt="icon" /> Encryption at rest (local storage &amp; DB)</td>
<td><img src="web-application-security.png" alt="icon" /> Web application security</td>
<td><img src="encryption-at-rest.png" alt="icon" /> Encryption at rest (local storage &amp; DB)</td>
</tr>
<tr>
<td><img src="os-and-application-hardening.png" alt="icon" /> OS and application hardening</td>
<td><img src="os-and-application-hardening.png" alt="icon" /> OS and application hardening</td>
<td><img src="identity-access-management.png" alt="icon" /> Identity &amp; Access Management</td>
</tr>
<tr>
<td><img src="identity-access-management.png" alt="icon" /> Identity &amp; Access Management</td>
<td></td>
<td><img src="identity-access-management.png" alt="icon" /> Identity &amp; Access Management</td>
</tr>
</tbody>
</table>
Data Security and Traceability

• Do you know exactly
  • Where your data is stored?
  • Who has access to your data?
  • Who is accessing your data?
  • If your data contains PII or other sensitive information?
  • If sensitive data is encrypted?
  • If stale/old data is deleted appropriately?
Data Security and Traceability

• e.g. AWS Storage:
  • Customers choose the region(s) in which their customer content will be stored.
Data Security and Traceability

- e.g. AWS Storage:
  - Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer’s chosen region(s),
Data Security and Traceability

- e.g. AWS Storage:
  - Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer’s chosen region(s), except as legally required
Data Security and Traceability

• e.g. AWS Storage:
  • Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer’s chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users.
Data Security and Traceability

• Most companies suffer from a fundamental lack of knowledge and insight about their data
• What they have, where it is, and who is accessing it
• Without this basic knowledge, the organization is left completely blind and exposed
• Preventing data loss requires you to become data-aware
  • To proactively find and secure your sensitive and confidential data before carelessness or a malicious act puts your data at risk
Data Security and Traceability

BACKUP, SNAPSHOT, AND TEST REGULARLY

Perform regular backups of all critical information, snapshot critical systems, and frequently test your ability to recover to limit the impact of data or system loss and to help expedite the recovery process.
Perform regular backups of all critical information, snapshot critical systems, and frequently test your ability to recover to limit the impact of data or system loss and to help expedite the recovery process.

Perform security monitoring for inappropriate or excessive use and perform spot audits to ensure compliance with departmental, state, and federal mandates.
Perform regular backups of all critical information, snapshot critical systems, and frequently test your ability to recover to limit the impact of data or system loss and to help expedite the recovery process.

Perform security monitoring for inappropriate or excessive use and perform spot audits to ensure compliance with departmental, state, and federal mandates.

Maintain a centralized mapping of where your sensitive data resides and who has (and does) access it.
QUANTIFY VALUE

Quantify the value of the data (not the asset) based on the content contained within the data and who has access to it.
Data Security and Traceability

QUANTIFY VALUE
Quantify the value of the data (not the asset) based on the content contained within the data and who has access to it.

DETERMINE PURPOSE
There is no room for sentimentality in data. Determine the business purpose of existing data and remove or archive legacy or unimportant data.

TIME

PEOPLE

CONTENT

VALUE

PURPOSE
QUANTIFY VALUE

Quantify the value of the data (not the asset) based on the content contained within the data and who has access to it.

DETERMINE PURPOSE

There is no room for sentimentality in data. Determine the business purpose of existing data and remove or archive legacy or unimportant data.
Regulatory Compliance & Governance

• “[abc] cloud provider is [xyz] compliant, so that means I am as well, right?”
• Unfortunately, this is all too common an assumption
• AWS’ shared responsibility model clarifies it quite well:

“Security and Compliance is a shared responsibility between AWS and the customer.”

ref: https://aws.amazon.com/compliance/shared-responsibility-model/
Regulatory Compliance & Governance

CUSTOMER

RESPONSIBLE FOR SECURITY “IN” THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY “OF” THE CLOUD

COMPUTE

STORAGE

DATABASE

NETWORKING

AWS GLOBAL INFRASTRUCTURE
www.leocybersecurity.com

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS
# Regulatory Compliance & Governance

<table>
<thead>
<tr>
<th>Certifications / Attestations</th>
<th>Laws, Regulations, and Privacy</th>
<th>Alignments / Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>C5 [Germany]</td>
<td>CISPE</td>
<td>CIS</td>
</tr>
<tr>
<td>Cyber Essentials Plus [UK]</td>
<td>EU Model Clauses</td>
<td>CJIS</td>
</tr>
<tr>
<td>DoD SRG</td>
<td>FERPA</td>
<td>CSA</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>GLBA</td>
<td>ENS [Spain]</td>
</tr>
<tr>
<td>FIPS</td>
<td>HIPAA</td>
<td>EU-US Privacy Shield</td>
</tr>
<tr>
<td>IRAP [Australia]</td>
<td>HITECH</td>
<td>FFIEC</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>IRS 1075</td>
<td>FISSC</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>ITAR</td>
<td>FISMA</td>
</tr>
<tr>
<td>ISO 27017</td>
<td>My Number Act [Japan]</td>
<td>G-Cloud [UK]</td>
</tr>
<tr>
<td>MTCS [Singapore]</td>
<td>VPAT / Section 508</td>
<td>ICERIA</td>
</tr>
<tr>
<td>PCI DSS Level 1</td>
<td>EU Data Protection Directive</td>
<td>IT Grundschutz [Germany]</td>
</tr>
<tr>
<td>SEC Rule 17-a-4(f)</td>
<td>Privacy Act [Australia]</td>
<td>MITA 3.0</td>
</tr>
<tr>
<td>SOC 1</td>
<td>Privacy Act [New Zealand]</td>
<td>MPAA</td>
</tr>
<tr>
<td>SOC 2</td>
<td>PDPA - 2010 [Malaysia]</td>
<td>NIST</td>
</tr>
<tr>
<td>SOC 3</td>
<td>PDPA - 2012 [Singapore]</td>
<td>PHR</td>
</tr>
<tr>
<td></td>
<td>PIPEDA [Canada]</td>
<td>Uptime Institute Tiers</td>
</tr>
<tr>
<td></td>
<td>Spanish DPA Authorization</td>
<td>UK Cloud Security Principles</td>
</tr>
</tbody>
</table>

[https://aws.amazon.com/compliance/]
Regulatory Compliance & Governance

- SSAE16 / ISAE 3402 Type II:
  - SOC 1, 2, and 3
- ISO 27001/27017/27018
- FedRAMP ATO for Google App Engine
- PCI DSS v3.2
- HIPAA
- CSA STAR
- MTCS Tier 3 Certification (Singapore)
- FISC (Japan)
- EU-U.S. & Swiss-U.S. Privacy Shield Frameworks

https://cloud.google.com/security/compliance
# Regulatory Compliance & Governance


<table>
<thead>
<tr>
<th>Filter by</th>
<th>Region</th>
<th>Country</th>
<th>Industry</th>
<th>Azure</th>
<th>Clear all</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina PDPA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina PDPA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIR 2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canadian Privacy Laws</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCSC (IRAP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOC 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain ENS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK Cyber Essentials PLUS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK G-Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WCAG 2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Argentina PDPA**: Microsoft has implemented the security measures in the Argentina Personal Data Protection Act.
- **BIR 2012**: Agencies operating in the Netherlands government sector must comply with the Baseline Informatiebeveiliging Rijksdienst standard.
- **Canadian Privacy Laws**: Microsoft contractually commits to implementing security that helps protect individuals’ privacy.
- **CCSC (IRAP)**: Microsoft is accredited for the Australian Certified Cloud Services List based on an IRAP assessment.
- **SOC 3**: Microsoft cloud services comply with Service Organization Controls standards for operational security.
- **Spain ENS**: Microsoft received Spain’s Esquema Nacional de Seguridad (National Security Framework) certification.
- **UK Cyber Essentials PLUS**: Cyber Essentials PLUS is a UK government-defined scheme to help organizations protect against common cyber-security threats.
- **UK G-Cloud**: The Crown Commercial Service renewed the Microsoft cloud services classification to Government Cloud v6.
- **WCAG 2.0**: Microsoft cloud services comply with the Web Content Accessibility Guidelines 2.0.
Summary

• There are many security challenges in cloud computing that make a lateral shift both an architectural and risk management exercise
• Though PaaS is quick and easy, it may not provide adequate security for the organization or allow it to meet its compliance objectives
• Just because the cloud infrastructure is compliant...doesn’t mean that you are as well
Thank You!

Questions?

Visit Us At:
https://www.leocybersecurity.com