Global Efforts to Secure Cloud Computing
Tech Consumerization: It’s all interconnected

- Cloud
- Smart Mobile
- Big Data
- Social
- Digital Natives
Key Trust Issues in cloud

- Transparency & visibility from providers
- Compatible laws across jurisdictions
- Data sovereignty
- Incomplete standards
- Lack true multi-tenant technologies & architecture
- Incomplete Identity Mgt implementations
- Risk Concentration
About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 39,000 individual members, 130 corporate members, 70 chapters
- Building security best practices for next generation IT
- Research and Educational Programs
- Cloud Provider Certification
- User Certification
- Awareness and Marketing
- The globally authoritative source for Trust in the Cloud

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”
Cloud as a layered model (eg OSI)

- SaaS has implicit IaaS layers

Market impacts architecture

- Businesses occupy individual layers

- Layers of abstraction emerge

- Innovation/optimization in layers

Everything becomes virtualized
Transparency

➢ Public visibility into Cloud Provider
➢ Corporate Governance
➢ Supply Chain
➢ Information Security Program
➢ Policies Impacting Customers
➢ Consumer right to know
➢ Public will demand better

*Sunlight is the best disinfectant,*” U.S. Supreme Court Justice Louis Brandeis
What hath Patriot Act wrought?

- USA Patriot Act “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and obstruct Terrorism Act of 2001” (reauthorized in 2006 & 2011)
- Not a new law, series of amendments to existing laws related to surveillance, investigation and prosecution of terrorism
- Most requests for information follow subpoenas/warrants
- National Security Letters
- Parallels to Patriot Act in many countries
- Convention on Cybercrime of the Council of Europe
- Canadian laws disclosing user info without user consent
  - Security Intelligence Service Act, Part II
  - Section 273.65 of the National Defence Act
  - Section 7 of PIPEDA
Government requests according to Google


- France: 29% increase in user data requests
- Germany: 39% increase in user data requests
- Spain: 28% increase in user data requests
- UK: 71% increase in content removal requests
- US: 70% increase in content removal requests
Cloud Data Governance Survey

- Cloud Data Governance WG
- Collaborative Working Group led by CSA Singapore and CSA Silicon Valley
  - Data Discovery
  - Location of Data
  - Data Aggregation or Inference
  - Commingling Data with Other Cloud Customers
  - Use of Data Security Controls
  - Data Encryption and Key Management
  - Data Backup and Recovery
  - Data Remanence and Persistence
Data Discovery

➡️ Ability to locate and search all customer data? 59%
   ➡️ Supervised search: 60%
   ➡️ Unsupervised search: 27%
   ➡️ Both: 13%

➡️ Many responses directly addresses multi-tenancy and partitioning of customer data from search

➡️ Overall, responses were diverse, reflecting the need for more prescriptive guidance on data discovery best practices
Location of Data

Does the CSP provide customer a specific location for storage and use of data? 82% said Yes

Technical enforcement of location? 73%

Separate location for backup/replication, still supporting customer legal concerns of location? 65%

CSPs understand this pain point and are addressing it, but more testing and documentation of assertions are needed
Does CSP provide capabilities to ensure that customer data can or cannot be aggregated according to requirements? 58% said Yes

Low level of maturity in this area, most positive responses were fortuitous based on their own models
Commingling Data with Other Cloud Customers

- Typical enforcement mechanisms
- Encryption of data for different users
- VLAN segregation
- Partitioning
- User/access rights controls
- Data classification and tagging
Use of Data Security Controls

- Governance framework for data security controls? 74%
- Third party audit of governance framework? 79%
- Customer audit of data security controls? 67%
- Sample controls
  - IP Ranges
  - ACLs
  - Logging
  - SCAP
- Greater adoption of CSA Cloud Controls Matrix and other frameworks needed
Data Encryption and Key Management

- Does the CSP provide end-to-end encryption? 84%
- Customer controlled capability to encrypt data at rest? 69%
- Formally vetted encryption algorithm for data at rest? 75%
- That last answer should be 100%!!!
Data Backup and Recovery

Does the CSP provide data backup services? 88%

Does the CSP allow location section for backup? 53%
Data Remanence and Persistence

Does the CSP delete data according to some identifiable standard? 33%

Typical responses
- Data is encrypted
- Media destruction in high assurance offerings
- Multi-pass disk rewrites

This is a poorly understood area
Reasons why private clouds are less secure than public

- Perimeter defenses obsolete
- Fixed or limited address space
- Innovation dilemma
- Inelastic deployment of compute in aid of security

Think about the agile bad guy…

- Exploits any technology, anywhere, anytime
- Legally exploiting any technology is the goal
What about Innovation?

- Grid, mobile clouds
- Brokers/ Virtual private clouds
- New devices, Internet of Things
- Communication hives, carrier bypass
- Dynamic, versionless software
- Security as a Service
- Thinking Virtually
Thinking Virtually

- Virtual OS
- Software-defined networking
- Virtual private clouds/DCs
- Migrate “para virtual” appliances to cloud blades
- Virtual SaaS
- Virtual countries
- Avatars

Key foundation: Instrumentation of entities (clouds, devices, data, instances, users) with robust identity mgt
Migrating to the Cloud

- Shared Responsibility
- Strategy
- Education
- Architecture / Framework
- Due Diligence

We are all cloud consumers, many of us are cloud providers

Copyright © 2012 Cloud Security Alliance
Global efforts

Governments
- EU Strategy released Sept 27
- NIST, FedRAMP

Standards bodies
- ISO SC 27
- ITU-T FG 17
- DMTF, PCI Standards Council

Private/Public
- Cloud Cities
- FP7, NSTIC, NSF
- Innovation
CSA GRC Stack

• Family of 4 research projects
  • Cloud Controls Matrix
  • Consensus Assessments Initiative
  • Cloud Audit
  • Cloud Trust Protocol
• Tools for governance, risk and compliance mgt
• Enabling automation and continuous monitoring of GRC
Path to high assurance

- Real time, continuous monitoring
- 3rd Party Assessment
- Self Assessment
- Clear GRC objectives

Cloud Trust Protocol (CTP) + Cloud Audit
CSA STAR Registry

- 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
- Security as a market differentiator
- www.cloudsecurityalliance.org/star
- The “Form 10-K” of Cloud Computing
## Consensus Assessments Initiative Questions

<table>
<thead>
<tr>
<th>Control Group</th>
<th>CGID</th>
<th>CID</th>
<th>Consensus Assessment Questions</th>
<th>Comments and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>DG-02</td>
<td>DG-02.1</td>
<td>Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., Tags can be used to limit guest operating)</td>
<td>2.1 - Yes, 2.2 - Yes, 2.3 - No, 2.4 - Yes, 2.5 - Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DG-02.2</td>
<td>Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DG-02.3</td>
<td>Do you have a capability to use system geographic location as an authentication factor?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DG-02.4</td>
<td>Can you provide the physical location/geography of storage of</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CCMv1.1 Compliance Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2012 Cloud Security Alliance
### DG 4.2: Do you have a documented procedure for responding to requests for tenant data from governments or third parties?

<table>
<thead>
<tr>
<th>Company</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon AWS</strong></td>
<td>AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.</td>
</tr>
<tr>
<td><strong>Box.net</strong></td>
<td>Box does have documented procedures for responding to requests for tenant data from governments and third parties.</td>
</tr>
<tr>
<td><strong>SHI</strong></td>
<td>Customer responsibility. SHI has no direct access, so requests for data through third parties will be responded to by the customer themselves, however, SHI can sanitize and delete customer data upon migration from the cloud.</td>
</tr>
<tr>
<td><strong>Verizon/Terremark</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>
CSA Open Certification Framework

- Leverage CSA STAR Infrastructure to create national, local or industry-specific provider certifications
- Allows governments, certification bodies and industry consortia to create certifications addressing specific requirements without developing complete & proprietary bodies of knowledge
- For those with unique certification requirements
- Leverage existing certification/attestation regimes
- Allows providers to certify once, comply many
- Program details announced Sept 25-26
Why Cloud Depends upon Identity

➢ Economics force efficiencies in compute utility

➢ Virtual controls become vital in asserting trust in shared world

➢ Robust Identity ecosystem enables virtual controls

www.cloudsecurityalliance.org
CSA Guidance – IAM Implementation

- CSA Security as a Service project
- Implementation Guides for 10 Categories
- IAM Guide released last week
- [https://cloudsecurityalliance.org/research/secaas/](https://cloudsecurityalliance.org/research/secaas/)

Research Sponsored By

- Ping Identity
- Courion™
Identity in the Cloud – Architecture

IAM Conceptual Capability Architecture
Identity in the Cloud – Implementation

- Provisioning lifecycle
- Multi-factor & risk-based authentication
- Directory Services & Synchronization
- Federated vs Web Single Sign-On
- Standards
- Fine-grained authorization
- Policy Management, logging, audit
Principles for moving forward

- Holistic IDs from Identity Providers (IdPs)
- CSPs should by default NOT be IdPs
- IAM must absolutely be applied to devices, data and applications as well as users
- Strong Authentication
- Identity “Net Neutrality”
- Enterprise role in providing identities
- Consumer activism

www.cloudsecurityalliance.org
CSA Mobile

- Securing application stores and other public entities deploying software to mobile devices
- Analysis of mobile security capabilities and features of key mobile operating systems
- Cloud-based management, provisioning, policy, and data management of mobile devices to achieve security objectives
- Guidelines for the mobile device security framework and mobile cloud architectures
- Solutions for resolving multiple usage roles related to BYOD, e.g. personal and business use of a common device
- Best practices for secure mobile application development

To be released at CSA Congress, Nov 7-8
MDM 17 key components

Mobile Threats (Evil 8 – Preliminary!)
1. Insecure or Rogue Marketplaces
2. Data Loss from Stolen, Lost, or Decommissioned Devices
3. Information Stealing Malware
4. Insecure WIFI / Network Access / Rogue Access Points
5. Insufficient Access to APIs, Management Tools, and Multi-Personas
6. Data Loss / Data Leaking Through Poorly Written Applications
7. Vulnerabilities in Hardware, OS, Applications, 3rd-Party Apps
8. NFC / Proximity-Based Hacking

BYOD Considerations
- Employee Privacy
- Legal Gray Areas: Overtime, Plan usage comp
- Compliance: What is allowed on device?
- Device Usage / Functionality / Onboarding
Our 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.
For More Information

- CSA Congress, Orlando, Nov 7-8
  - www.misti.com/cloud

- Research
  - https://cloudsecurityalliance.org/research/grc-stack/

- How much do you know about cloud security?
  - https://cloudsecurityalliance.orf/certifyme

- Provider Registry of Security Practices
  - https://cloudsecurityalliance.org/star/
Summary

- Cloud, tech consumerization unstoppable forces
- Pragmatic adoption based on tools available and cloud models
- Think Virtually
- Demand Transparency!
- Dialogue/Debate on Identity Principles
- Must be holistic, mobile, SDN, etc

www.cloudsecurityalliance.org/
THANK YOU

cloud security alliance™