Cloud Computing Governance & Security

Security Risks in the Cloud
The top ten questions you have to ask

Mike Small CEng, FBCS, CITP
Fellow Analyst, KuppingerCole

This Webinar is supported by Novell.
Agenda

☐ What is the Problem?
☐ Ten Cloud Security Questions to Ask
☐ Summary
WHAT’S THE PROBLEM?
Cloud – Top Security Benefits

- **Benefits of Scale**
  - The same investment buys better protection

- **Standard Interfaces for Security Services**
  - Creates a more open market for security services.

- **Rapid, smart scaling of resources**
  - Dynamic reallocation of resources improves resilience.

- **Audit and Evidence Gathering**
  - provide dedicated, pay-per-use forensic images of VMs

- **Better updates and defaults**
  - Default VM images with best configuration and patches

Cloud – Top Threats

ENISA Cloud Risk Assessment
- Loss of Governance
- Compliance Challenges
- Changes of Jurisdiction
- Isolation Failure
- Cloud provider – malicious insider – privilege abuse
- Management Interface compromise
- Data Deletion Risks
- Network Management

Cloud Security Alliance - Top Threats
- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking

ENISA - Cloud Computing - Benefits, risks and recommendations for information security

Cloud Security Alliance - Top Threats to Cloud Computing V1.0
# Risk - Who is responsible?

<table>
<thead>
<tr>
<th></th>
<th><strong>Customer</strong></th>
<th><strong>Cloud Provider</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness of content</td>
<td>Full liability</td>
<td>Intermediary liability</td>
</tr>
<tr>
<td>European Data Protection Law status</td>
<td>Data Controller</td>
<td>Data Processor (external)</td>
</tr>
<tr>
<td>Identity &amp; Authentication</td>
<td>Own users and federation agreements with partners</td>
<td>Users required to manage the provided infrastructure</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Own infrastructure</td>
<td>Cloud service infrastructure (server, storage, bandwidth etc)</td>
</tr>
<tr>
<td>Security Management</td>
<td>Guest systems (IaaS)</td>
<td>Host systems and applications security policy, hardening, patching and monitoring</td>
</tr>
</tbody>
</table>
Cloud - Managing Risk

- Due Diligence by Customer
  - Ask Questions
  - Fully specify Security Service Levels

- Clear Division of Liabilities
  - Example: Customer = Data Controller, Provider = Data Processor (External)

- Clear Division of Responsibilities
  - Depends upon Service Model (SaaS, PaaS or IaaS)

- Certification of Providers
TEN CLOUD SECURITY QUESTIONS TO ASK
Q1: How is Identity and Access Managed in the Cloud?
Risk: Impersonation

Google Apps Security Questioned After Twitter Leak.
Seth H. Weintraub, Computerworld
Jul 17, 2009
Analysis: Twitter suffers a significant security breach, brought on by a Twitter employee's Google Apps account being hacked.

According to Twitter founder Ev Williams:
"Yes, we did suffer an attack a few weeks ago and are familiar with this list of stuff. This is unrelated to the hack of Twitter where someone gained access to users' accounts. This had nothing to do with the security of Twitter.com, and there were no user accounts compromised here...

This isn't to say that Google Apps has weak security. The security of Google Apps is what you make of it. This employee probably had a weak password...."
Risk: Management Interface

ISO 27001 Control 11.2:

- **Objective:** To ensure authorized user access and to prevent unauthorized access to information systems. Risk – management interface compromise.

- **Questions:**
  - What extra security is provided to protect remote management capabilities?
  - What forms of authentication are used for management interfaces?
  - How is the management interface monitored?
Identity Federation

Federation makes it possible to use the organizational identity service to access the Cloud service:

- A Trusted Identity Provider makes a “claim” of identity to the Cloud system which relies upon this claim.
- This is similar to a citizen of one country using a passport to enter another country.

ISO 27001 Control 11.2:

- [Image: Diagram showing the relationship between Identity Provider, Federation Infrastructure, Business Owner, User, and Relying Party.]
Key Questions: Your Identity and Access

- **Key questions for the provider:**
  - Does the system allow for a federated IDM infrastructure which is interoperable both for high assurance and low assurance (e.g., username and password)?
  - Is the cloud provider interoperable with third party identity providers?
  - Is there the ability to incorporate single sign-on?
  - Does the client credential system allow for the separation of roles and responsibilities?
  - Is there mutual authentication?

ISO 27001 Control 11.2:
Q2: Where will my data be geographically located?
Legal Risk: Data Protection

Zurich Insurance fined £2.3m over customers' data loss [www.news.bbc.co.uk]

Aug 24th, 2010

The UK operation of Zurich Insurance has been fined personal details of 46,000 customers, the Financial Services Authority. The data on policyholders, including in some cases bank account and credit card information, went missing in August 2008.

However, Zurich did not become aware of the loss until a year later when it then began notifying customers.

The information went missing during a routine transfer to a centre in South Africa.

The FSA said in a statement: "Zurich UK failed to take reasonable steps to ensure it had effective systems and controls to manage the security of customer data resulting from the outsourcing arrangement."
Key Questions – Data Location

ISO 27001 Control 15.1.4:

- Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
- Key Questions:
  - In what country is the cloud provider located?
  - Where is the cloud provider’s infrastructure located?
  - Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider?
  - Where will the data be physically located?
  - Will any of the cloud provider’s services be subcontracted out or outsourced?
  - What happens to the data upon termination of the contract?
  - Do you rely on data dispersal algorithms?
Q3: How securely is my data handled?
Microsoft recovers Sidekick data
www.news.bbc.co.uk
Oct 15, 2009

Microsoft says it has now recovered the personal data lost when its Sidekick servers suffered an outage on 13 October.

The online service backs up contacts, photos, calendar appointments and other personal data stored on the mobile phones of Sidekick T Mobile customers.

Microsoft Corporate Vice President Roz Ho says that all data will be restored, beginning with personal contacts.

She believes that only a minority of Sidekick users are still affected. "The outage was caused by a system failure that created data loss in the core database and the back up," she wrote in an open letter to customers.

The issue has been seen by industry experts as the largest failing for cloud computing in recent memory.
Risk: Ineffective Data Deletion

Missile data found on hard drives

www.news.bbc.co.uk
May 17, 2009

Sensitive information for shooting down intercontinental missiles as well as bank details and NHS records was found on old computers, researchers say.

Of 300 hard disks bought randomly at computer fairs and an online auction site, 34% still held personal data.

Researchers from BT and the University of Glamorgan bought disks from the UK, America, Germany, France and Australia.

The information was enough to expose individuals and firms to fraud and identity theft, said the researchers.

Professor Andrew Blyth said: "It's not rocket science - we used standard tools to analyse the data".
Key Questions: Media Handling – Backup and Deletion

ISO 27001 Control 10.7:

- To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruptions to business activities.

- Can the Provider:
  - Detail policies and procedures for backup?
  - These should include procedures for the management of removable ...
  - Detail the steps taken to ensure that data which has been deleted is completely wiped and cannot be accessed by other service users.
  - Ensure that devices containing sensitive information are physically destroyed or overwritten using techniques to make the original information non-retrievable.
Q4: How is access by privileged users controlled?
Risk: Abuse of High Privilege Role

Admin Who Kept San Francisco Network Passwords Found Guilty

www.pcworld.com
April 28, 2010

the San Francisco network administrator who refused to hand over passwords to his boss, was found guilty of one felony count of denying computer services, a jury found.

Although the city's network continued to run, San Francisco went 12 days without administrative control of the FiberWAN, and that constituted a denial of service – illegal under state law.
Key Questions: Provider Identity & Access

ISO 27001 Control 11.2:

- Questions for providers on managing their privileged identities:
  - What checks are made on the identity of users with privileged access?
  - Are there different levels of identity checks based on the resources accessed?
  - What processes are in place for de-provisioning privileged credentials?
  - Are privileged credentials provisioned and de-provisioned simultaneously throughout the cloud system.
Q5: How is my data protected against privileged user abuse?
Risk: Abuse of High Privilege Role

Database admin steals 2.3M consumer records at Fidelity National subsidiary

A senior database administrator at a subsidiary of Fidelity National Information Services Inc. who was responsible for defining and enforcing data access rights at the company instead took data belonging to about 2.3 million consumers and sold it to a data broker.

Computer World, July 3rd, 2007

The broker in turn sold a subset of the data to other marketing companies. The stolen data included names, addresses, birth dates, bank account and credit card information, the company said in a statement released today.
Key Questions: Privileged Access Controls

ISO 27001 Control 11.2.2:

- The allocation and use of privileges should be restricted and controlled.
- **Questions for the provider.**
  - *Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations?*
  - *How are the accounts with the highest level of privilege authenticated and managed?*
  - *How are privileged actions monitored and logged?*
Key Questions: Segregation of Duties

ISO 27001 Control 10.1:

- Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

- **Questions for the provider:**
  - Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?
  - Do you use role-based access control (RBAC)?
  - Is the principle of least privilege followed?
Key Questions: Monitoring User of Privilege

ISO 27001 Control 10.10.2:

- Procedures for monitoring use of information processing facilities should be established...
  ...especially all privileged operations.
- Can the provider detail?
  - How are privileged actions monitored and logged?
  - What recorded events result in action being taken?
  - What controls are employed to protect logs from unauthorised access or tampering?
  - What method is used to check and protect the integrity of audit logs?
Q6: What levels of isolation are supported?
Risk: Isolation Failure

- "This class of risk includes the failure of mechanisms separating storage, memory, routing and even reputation between different tenants.

- Malicious activities carried out by one tenant may affect the reputation of another tenant. The impact can be a loss of valuable or sensitive data, reputation damage and service interruption for cloud providers and their clients."

<table>
<thead>
<tr>
<th>Probability</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Key Questions: Separation/Isolation

ISO 27001 Control 11.6.2:

- Sensitive systems should have a dedicated (isolated) computing environment.

- Questions for the provider:
  - What levels of isolation are used for virtual machines, physical machines, network, storage, management networks and management support systems, etc.
  - Provide information on how multi-tenanted applications are isolated from each other.
Q7: How is my data protected in virtual environments?
Risks - Virtualization

- PCI DSS specifies “one function per server”. This is taken by some auditors to limit virtualization.
- A VM Image is completely transportable and can be installed on any machine!

<table>
<thead>
<tr>
<th>Probability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Source: Payment Card Industries Data Security Standard.
Key Questions: Protection of VM Images

ISO 27001 Control 10.7:

- Appropriate operating procedures should be established to protect documents, computer media, ..from unauthorized disclosure, modification, removal, and destruction.

- Questions:
  - Are virtual images hardened by default?
  - Is the hardened virtual image protected from unauthorized access?
  - Confirm that the virtualised image does not contain the authentication credentials?
Q8: How are the systems protected against internet threats?
Risk: Economic Denial of Service

Bot herders hide master control channel in Google cloud

By Dan Goodin in San Francisco

Cyber criminals' love affair with cloud computing just got steamier with the discovery that Google's AppEngine was tapped to act as the master control channel that feeds commands to large networks of infected computers.

The custom application was used to relay download commands to PCs that had already been infected and made part of a botnet, said Jose Nazario, the manager of security research at Arbor Networks. Google shut down the rogue app shortly after being notified of it....

Researchers from Symantec found a Facebook account pumping commands to zombie drones. And in August, Nazario found several Twitter accounts that were doing much the same thing.
ISO 27001 Control 10.6.2:

- Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement.

- **Questions for the provider:**
  - Define the controls used to mitigate DDoS (distributed denial-of-service) attacks.
  - Do you have defences against internal as well as external threats?
  - Does architecture support continuous operation?
  - Is the network infrastructure secured to best practice specific standards (e.g., are MAC spoofing, ARP poisoning attacks, etc, prevented)
Q9: How are activities monitored and logged?
Risk: Loss or Compromise of Logs

The Athens Affair.
IEEE Specturm
By Vassilis Prevelakis, Diomidis Spinellis // July 2007

"Just as we cannot now know for certain who was behind the Athens affair or what their motives were, we can only speculate about various approaches that the intruders may have followed to carry out their attack. That's because key material has been lost or was never collected. For instance, in July 2005, while the investigation was taking place, Vodafone upgraded two of the three servers used for accessing the exchange management system. This upgrade wiped out the access logs and, contrary to company policy, no backups were retained."
Key Questions: Monitoring and Logging

ISO 27001 Control 10.10:

- Systems should be monitored and information security events should be recorded.

- Can the provider detail:
  - What information is recorded in audit logs?
  - For what period is this data retained?
  - How data is segmented within audit logs so they can be made available to the end customer and/or law enforcement without compromising other customers?
  - How are audit logs reviewed? What recorded events result in action being taken?
  - How is accurate event time stamping provided?
Q10: What kind of information security certification do you have?
Risk:
Loss of Governance

“Certain organizations migrating to cloud have made considerable investments in achieving certification either for competitive advantage or regulatory requirements – (e.g. PCI DSS)”

<table>
<thead>
<tr>
<th>Probability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>High</td>
</tr>
</tbody>
</table>
Best Practice and Certification

- Does the Cloud provider comply with best practice? Are they certified?

- CSA Mapping of Cloud Best Practice to:
  - COBIT, ISO/IEC 27002-5, NIST SP800-53, PCI-DSS
    Cloud Security Alliance Cloud Controls Matrix
  - CSA (CCSK) Certificate of Cloud Security Knowledge
    [Cloud Security Alliance Certificate of Cloud Security Knowledge](http://www.cloudsecurityalliance.org/certifyme.html)
Summary

- **Key Risks**
  - CSA and ENISA Risk Assessments
- **Managing Risk in the Cloud**
  - Due Diligence by Customer
  - Clear Division of Liabilities
  - Clear Division of Responsibilities
  - Certification of Providers
- **Ten Key Questions to Ask**
For More Information

Mike Small CEng, FBCS, CITP
Fellow Analyst

Email: Mike.Small@kuppingercole.com
Mobile: +44 7777 697 300
QUESTIONS?