Cloud Security Strategies

Fabio Gianotti, Head of Cyber Security and Enterprise Security Systems

London, 14 October 2015
UNICREDIT AT A GLANCE

- Employees: more than 146,600
- Branches: 8,403
- Banking operations in 17 countries
- International network spanning: ~50 countries
- Global player in asset management: €221 bn in managed assets
- Market leader in Central and Eastern Europe leveraging on the region's structural strengths
A COMPLEXITY TO BE MANAGED
The approach to ICT Security Governance follows different paths

- UniCredit landscape is complex
- Different country regulations
- Different approaches to cloud adoption due to high-number and the geographical distribution of UniCredit Data Centers
- Cloud adoption strategy for Data Centers consolidation framework, and Business Enabler
- Strong ICT Security governance is both mandatory and strongly recommended

Last but not least:
Judgment of European Court of Justice in CASE C-362/14 declaring the Commission's US Safe Harbor Decision invalid. . . . . any Ideas from ENISA team?
WHERE CLOUD DATA ARE LOCATED AND WHICH LAW IS APPLIED
Several components to be addressed (in order to set a comprehensive Cloud security strategy)

**Cloud Security Strategy**
A comprehensive program and strategy to embed security throughout the enterprise’s cloud lifecycle with Security Dashboard monitoring

**Integration**
- Interoperability
- Lock in / portability
- Security Analytics
- Administration console
- Public / Private / Hybrid models
- Secure connection to other systems and data
- Event Management

**Platform & Software Applications**
- Threat and vulnerability identification / Access Control
- Monitoring / Management
- Application vulnerability management and remediation

**Data**
- Data Classification
- Data Backup, Retention
- Data Ownership, Segregation
- Risk Assessments
- Encryption / Tokenization
- Data loss prevention
- Secure storage, secure disposal
- Audit and forensics

**Users & Identity**
- Roles and authorization levels and authentication
- Evaluation / monitoring of usage patterns
- Program awareness and education

**Infrastructure**
- Security functionality
- Network configuration
- Cloud hardening
- Vulnerability management
- Infrastructure operations

**Governance**
- Define processes and policies (ownership, connectivity, privacy, audit / wipe)
- Legal (NDA, SLA, licensing)
- Audit and Compliance
- Identify preferred suppliers / service level for business
- Business Continuity
- Training & Awareness
### Summary of scoring results

<table>
<thead>
<tr>
<th>Clusters</th>
<th>ACME</th>
<th>Best Provider</th>
<th>Provider 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit &amp; Compliance</td>
<td>11.5</td>
<td>11.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Application Security Testing</td>
<td>5.0</td>
<td>5.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>10.0</td>
<td>6.5</td>
<td>0.0</td>
</tr>
<tr>
<td>Cloud Hardening</td>
<td>10.0</td>
<td>6.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Encryption &amp; Tokenization</td>
<td>5.0</td>
<td>15.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Governance</td>
<td>10.0</td>
<td>5.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Interoperability</td>
<td>0.0</td>
<td>2.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Identity &amp; Access Management</td>
<td>6.5</td>
<td>7.5</td>
<td>0.0</td>
</tr>
<tr>
<td>Information Management (Data Protection)</td>
<td>4.4</td>
<td>5.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Infrastructure Operations</td>
<td>10.0</td>
<td>6.4</td>
<td>0.0</td>
</tr>
<tr>
<td>Legal</td>
<td>8.6</td>
<td>7.3</td>
<td>0.0</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>7.5</td>
<td>5.5</td>
<td>0.0</td>
</tr>
<tr>
<td>Portability</td>
<td>10.0</td>
<td>6.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Physical Security</td>
<td>8.8</td>
<td>6.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>8.8</td>
<td>6.8</td>
<td>0.0</td>
</tr>
<tr>
<td>Security Incident &amp; Event Management</td>
<td>8.0</td>
<td>3.4</td>
<td>0.0</td>
</tr>
<tr>
<td><strong>Total Score</strong></td>
<td><strong>125.0</strong></td>
<td><strong>119.7</strong></td>
<td><strong>0.0</strong></td>
</tr>
</tbody>
</table>
IS THERE ANY DIFFERENCE BETWEEN DATA AND THEIR APPLICATIONS IN THE CLOUD?

- Yes, the law is applied to the data, not to the application
- If you can encrypt the data, then the cloud provider has no access to the data. This might change how responsibilities are allocated from a compliance point of view according to the countries where your business is.
• Cloud Ready overview declines the Group CIO Global and Group CIO ICT Security cloud strategy and feasibility, in order to design a sustainable and common UniCredit Service Platform/Framework.

• Cloud computing is a new way of delivering computing & services resources, not a new technology. Computing services ranging from data storage and process to software on demand to launch new time-to-market business proposition in UniCredit multichannel perspective.

• The massive concentrations of resources and data could represent a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective in terms of IT security perspective.

• It is important to note that cloud computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Lastly API rest exposure, for B to B and B to C customers services.
FINAL TAKE-AWAYS

- Cloud benefits in terms of elasticity, scalability, on-demand computing power – growing list of providers

- Companies must be structured (or re-structured) in order to deal with a new generation of risk evaluation, and address the best cloud strategic and omni-comprehensive approach (data protection, application security, network security, encryption, file sharing, local and global regulation, compliance, log management, identity management, KPI & SLA, etc), in order to deploy a strong and sustainable security governance.

- Companies must raise the bar on ongoing security activities, while addressing at least three key-points to the respective cloud provider:
  - Setting the minimum security level expected
  - Managing the increasing complexity with different and new monitoring points
  - Putting on the table technical skills, more and more sophisticated with a holistic view

- Bridging the gap between requirements, risks and skills

Fabio.gianotti@unicredit.eu