Cloud Computing - Cyber Security Challenges for the Finance Sector

Dr. Evangelos Ouzounis
Head of Unit – Secure Infrastructures and Services - ENISA
Positioning ENISA activities
## Cloud Opportunities for Finance Sector

<table>
<thead>
<tr>
<th>Economies of Scale</th>
<th>Support innovation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Better ROI</td>
<td>• Easier deployment of new services</td>
</tr>
<tr>
<td>• More efficient resource utilization also means cost savings</td>
<td>• Faster time to market</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Resiliency</th>
<th>Standardised solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Better back up services</td>
<td>• Better patch management</td>
</tr>
<tr>
<td>• Better business continuity</td>
<td>• Better software update management</td>
</tr>
<tr>
<td></td>
<td>• Portable and interoperable</td>
</tr>
</tbody>
</table>
Cloud Challenges for Finance Sector

Isolation Failures
- One Cloud customer might be able to influence the resources of another (CPU, Memory)
- or have access to another customers’ data (data breach)

Loss of Governance
- Control sufficiently the resources in the Cloud
- This also affects security

Compliance Risks
- Provide enough evidence for taking care of data
- Prove prudent risk management practices

Vendor Lock-in
- Always have exit strategy
- Properly remove the data from the Cloud
Objectives of the study

- Identify the status on cloud adoption in EU and elsewhere
- Identify good practices at technical and policy level
- Recommend good practices to be used by banks and regulators
- Propose recommendations to policy makers, banks and Cloud providers
Cloud Adoption - Status

• Existing regulations and policies focus on finance core operations and do not cover sufficiently cloud cyber security

• Challenges with data jurisdiction and data protection rules

• Not enough understanding/knowledge on cloud challenges by regulatory authorities

• Unclear regulatory and policy environment makes difficult deployment of Cloud for financial institutions

• Many standards in the cloud area complicate both financial institutions and regulators to deploy cloud, as none of them is widely accepted

• ad-hoc implementations focus on clouds in non-core business; limited strategic view
Has your Financial Institution developed a detailed corporate risk assessment for Cloud Computing?
Main challenges to cloud computing

1. Regulatory obligations for data retention and archival
   - CSP: 58%
   - FI: 33%
2. Logs collections and analysis (e.g., for Security Incidents detection, analysis and response)
   - CSP: 0%
   - FI: 29%
3. Integrated Platforms (e.g., ERPs)
   - CSP: 29%
   - FI: 33%
4. The migration of EDW (Enterprise Data Warehouse) to Big Data/Cloud-based EDW
   - CSP: 0%
   - FI: 17%
5. Disaster Recovery / Business Continuity
   - CSP: 8%
6. High Frequency Trading solutions
   - CSP: 0%
   - FI: 100%
7. Other
   - CSP: 25%
   - FI: 33%
Which regulations mainly impact Cloud adoption?
How do you ensure compliance?

- Specific clauses in the contract (e.g. right to audit): 92% (CSP), 67% (FI)
- SLA: 83% (CSP), 100% (FI)
- Certification: 71% (CSP), 100% (FI)
- Other: 29% (CSP), 33% (FI)
Recommendations

Cooperation between FIs, NFSA and CSPs
- Good practices and guidelines in the area of Cloud security
- EU wide harmonization of legal and regulatory requirements

Risk assessment and cloud strategy
- FI to develop a corporate risk assessment and strategy for deploying Cloud

Transparency & Assurance
- CSPs to provide proven evidence of good cyber practices (incident handling, resilience, .. ) in use

Awareness campaigns
- FI, NFSA and CSP to co-operate on bridging the knowledge and awareness gap on cyber security of cloud
Next Steps

• ENISA remains ready to:
  - Provide more expert support where useful and needed to address the identified challenges
  - Continue as a catalyst for the needed information exchange, cooperation and discussions between FIs, regulators and CSPs
  - Continue the established cooperation with the regulatory authorities
Co-operation with other initiatives

• The SecuRe Pay (Security of Retail Payment Systems) working group, namely
  - secure communication,
  - secure customer authentication
  - incident reporting

• The Task Force on IT Risk Supervision
  - Transversal IT risk identification and analysis
  - IT risk and experiences - Cloud computing
  - Guidelines on the assessment of IT risk
  - Cooperation and training
Conclusions

- cloud modernizes the Financial Sector and achieves significant business benefits
- cyber security is key enabler for the smooth cloud adoption
- existing policies and regulations do not cover fully cyber security challenges related to cloud
- policy makers are not fully aware of the major cyber security challenges
- Plethora of good practices on cloud but not focused on finance sector
- limited information sharing among public and private sector on major cloud incidents affecting finance sector

ENISA will co-operate with policy makers (e.g. EBA, NFSAs) & private sector (e.g. banks, cloud providers) to accelerate cloud adoption in the finance sector
Thank you

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu