Study on Cloud security in Japan

2011/February

Professor Yonosuke HARADA
INSTITUTE of INFORMATION SECURITY
Content

1 Background
2 Survey
   2.1 Respondents
   2.2 User on cloud services
   2.3 Risk issues for Cloud computing
   2.4 User selection of Cloud provider
3 Comparison with the study by ENISA
4 Conclusion
Institute of Information Security conducted a survey for use of cloud computing survey to companies, government and universities.

One major purpose is to compare risk attitude of ENISA “Cloud Computing Risk Assessment”.

Survey term: 2010 August 1st to 31st
Survey by: mail
Target: Companies, government (local and central), Universities, 4,500
Effective Answer: 316 (7%)

Main survey items:
(1) Organization (size, employees, Sales, and PCs)
(2) Intention against cloud computing
(3) Risk evaluation for cloud computing
(4) Selection criteria for cloud provider
2.1 Respondent

Answer Divisions (N=315)

- Information Security Dev.: 63%
- General Dev.: 17%
- Other Dev.: 6%
- Information Systems Dev.: 5%
- Planning Dev.: 4%
- Business Dev.: 1%
- Secretary of CEO: 1%
- Finance Dev.: 1%
- HR Dev.: 3%
- Other: 3%
2.1 Respondent 2

Respondent Position (N=312)

- 34% Manager
- 20% Directors
- 19% Chief
- 16% Staff
- 4% President
- 3% President
- 2% Others
- 1% Specials
- 1% BU Director
2.1 Respondent 3

Respondent Industry (N=313)

- Manufacturer: 33%
- Retail, Wholesale: 12%
- University: 8%
- Construction: 8%
- Information Processing: 8%
- Government (central, local): 4%
- Others: 4%
- Transportation: 3%
- Service, Entertainment, Toiletry, Hotel, Dining: 3%
- Medical, Welfare: 3%
- Agriculture, Forestry, Fishery, Mining: 3%
- Real estate, Leasing: 2%
- Financial, Securities: 1%
- Real estate, Leasing: 1%
- Government (central, local): 1%
- University: 1%
- Construction: 1%
- Information Processing: 1%
- Retail, Wholesale: 1%
- Manufacturer: 1%
- Others: 1%
- Real estate, Leasing: 1%
2.1 Respondent 4

Annual Sales

- Less than 1bil Yen: 3%
- 1bil – 3bil Yen: 1%
- 3bil – 5bil Yen: 2%
- 5bil – 10bil Yen: 4%
- 10bil – 50bil Yen: 17%
- 50bil – 100bil Yen: 16%
- 100bil – 300bil Yen: 6%
- 300bil – 500bil Yen: 9%
- 500bil – 1,000bil Yen: 13%
- No (Non-profit, government): 27%

(N=309)
2.1 Respondent 5

Number of Employees (N=315)

- Less than 100: 15%
- 100-299: 19%
- 300-499: 16%
- 500-999: 24%
- 1,000-1,499: 8%
- 1,500-4,499: 12%
- 5,000-9,999: 4%
- 10,000-49,999: 2%
- 50,000-: 4%
2.1 Respondent 6

Number of PCs (N=314)

- Less than 1%: 3%
- 100-299: 5%
- 300-499: 16%
- 500-999: 16%
- 1,000-1,499: 26%
- 1,500-4,999: 14%
- 5,000-9,999: 8%
- 10,000-49,999: 12%
- 50,000-: 12%

- Less than 100
- 100-299
- 300-499
- 500-999
- 1,000-1,499
- 1,500-4,999
- 5,000-9,999
- 10,000-49,999
- 50,000-
2.1 Respondent 7

Security Policy (N=315)

- Developed: 76%
- Under Developing: 12%
- No: 12%
2.1 Respondent 8

IT audit for cloud computing (N=316)

What sort of IT audit do you have had last year?

- Internal audit: 151
- No audit: 135
- External audit: 59
- ISMS Internal audit: 28
- Internal audit for Privacy Certification: 27
- Internal audit for PCI-DSS: 1
2.1 Respondent 9

Security Incident and frequency  (N=312)

- Never: 65%
- Experienced in the past: 28%
- One time in a year: 3%
- 2-4 times in a year: 1%
- 5-9 times in a year: 1%
- More than 10 times in a year: 2%
2.2 Cloud computing 1

Usage of Cloud Computing （N=315）

- Using: 33%
- Under planning: 20%
- No plan but hope to use in the near future: 6%
- No plan and no need at this point: 41%

20% used and additionally 48% is willing to use
2.2 Cloud computing 2

Cloud Provider adoption (N=316)
Which cloud provider are you selected or going to adopt?

- Big Japanese provider: 113
- Private Cloud: 49
- Medium and small Japanese provider: 42
- Google: 33
- Telecomm Operator: 28
- Salesforce.com: 23
- Others: 17
- Provider within a Group: 11
- Other overseas provider: 9
- Amazon Web Services: 6
2.2 Cloud computing 3

Service selection  (N=316) multiple answer

Which kind of cloud services are you selected or going to adopt?

- SaaS (Software as a Service) - 164
- PaaS (Platform as a Service) - 67
- IaaS (Infrastructure as a Service) - 62
2.2 Cloud computing

Which is bigger threat? (N=311)
(1) Information Systems (under control) or cloud computing
(2) Outsourcing (including Hosting) or cloud computing

Users feel a little bigger threat in Cloud computing than IS under control or outsourcer. However, many think similar threat.
2.3 Cloud computing provider adoption 1

Important items are for provider adoption
Top five items are listed (N=316)

1. Incident response
2. Monthly charge
3. Technical support
4. Initial Cost is low
5. Technical Experience

- Most important
- Very Important
- Important
- Not so important
- Not at all
2.3 Cloud computing provider adoption 2

Important items are for provider selection
Bottom five items are listed (N=316)

1. Advertisement
2. Seminar or events
3. Brand name
4. Proposals
5. Selection of

![Chart showing importance levels of provider selection criteria](chart.png)
2.3 Cloud computing provider adoption

User Satisfaction
Top five items are listed (N=70)

1. Company profile
2. Initial charge
3. Company experience
4. Incident Response
5. Technical Experience

- Very satisfied
- Satisfied
- Not so satisfied
- Unsatisfied
- Very unsatisfied

Company profile: Very satisfied, Satisfied, Not so satisfied
Initial charge: Very satisfied, Satisfied, Not so satisfied
Company experience: Very satisfied, Satisfied, Not so satisfied
Incident Response: Very satisfied, Satisfied, Not so satisfied, Unsatisfied
Technical Experience: Very satisfied, Satisfied, Not so satisfied, Unsatisfied
2.3 Cloud computing provider adoption 4

Satisfaction on Cloud Service Used
Top five “unsatisfied” items are listed (N=70)

1. Speedy implementation
2. Quality of Proposal
3. Reasonable Running Cost
4. Reporting for Service
5. Audit

Users require provider proposal of cloud service
Some user does not satisfy current service
2.3 Cloud computing provider adoption

Cloud provider SLA

Top ten SLA items for adoption of cloud provider (N=316) multiple answer

1. Alternative service of major incident
2. Service up time
3. Average recovery time
4. Service Availability
5. Service hours (help desk etc.)
6. Backups methodology
7. Retention Period of backups
8. Average response time
9. Logging capability
10. Fault reporting process

ITGI Japan
Third party certification of guideline

(N=316) multiple answer

1. ISMS certification
2. Privacy certification (domestic)
3. BS25999 (BCM) certification (BSI)
4. Disclosure for ASP/SaaS service
5. SAS70-type2 and similar by CPA
6. PCIDSS certification
7. SysTrust certification
8. CSA guidelines
9. Others
### Organizational Risk 1

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOCK-IN</strong></td>
<td>High</td>
</tr>
<tr>
<td>Data format for storage, conversion tool is not provided Application lock-in</td>
<td></td>
</tr>
<tr>
<td><strong>LOSS OF GOVERNANCE</strong></td>
<td>High</td>
</tr>
<tr>
<td>All business processes are under control of Cloud Provider and cannot change or manage by user</td>
<td></td>
</tr>
<tr>
<td><strong>COMPLIANCE CHALLENGES</strong></td>
<td>High</td>
</tr>
<tr>
<td>If cloud provider violate laws and regulations, user may automatically challenge compliance.</td>
<td></td>
</tr>
<tr>
<td><strong>LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Business competitiveness may harm because of user reputation will become no difference based on cloud service</td>
<td></td>
</tr>
</tbody>
</table>

Survey result shows percentage of risk assessment by respondent

Japanese organisations do not think that “Lock in”, “Loss of governance” and “Compliance” are not so serious for their business.
### Organizational Risk 2

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLOUD SERVICE TERMINATION OR FAILURE</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Organization may not continue service, if cloud provider stops operation or service.</td>
<td></td>
</tr>
<tr>
<td><strong>CLOUD PROVIDER ACQUISITION</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Cloud provider is acquired by competitor and may not continue service.</td>
<td></td>
</tr>
<tr>
<td><strong>SUPPLY CHAIN FAILURE</strong></td>
<td>Low</td>
</tr>
<tr>
<td>Cloud service may stop or change due to changes or outage of other cloud service provider.</td>
<td></td>
</tr>
</tbody>
</table>

![Survey Result Diagram]

Japanese organisations thinks it more serious on service continuation than EU organization. However, they are optimistic on acquisition.
3 Comparison with ENISA result (2)

Technical Risk 1

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESOURCE EXHAUSTION</td>
<td>Medium</td>
</tr>
<tr>
<td>Inaccurate modeling of resources or inaccurate resources allocation algorithms may degrade service</td>
<td></td>
</tr>
<tr>
<td>ISOLATION FAILURE</td>
<td>High</td>
</tr>
<tr>
<td>Failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure</td>
<td></td>
</tr>
<tr>
<td>CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES</td>
<td>High</td>
</tr>
<tr>
<td>The malicious activities of an insider could potentially have an impact on all kind of services, and therefore indirectly on the organization’s reputation.</td>
<td></td>
</tr>
<tr>
<td>MANAGEMENT INTERFACE COMPROMISE</td>
<td>Medium</td>
</tr>
<tr>
<td>Customer management interfaces are Internet accessible and increased risk when combined with remote access and web browser vulnerabilities.</td>
<td></td>
</tr>
</tbody>
</table>

Japanese users feel “Malicious insider abuse” like EU but do not feel seriously for isolation failure.
## 3 Comparison with ENISA result (2)

### Technical Risk 2

<table>
<thead>
<tr>
<th>リスク</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERCEPTING DATA IN TRANSIT DATA LEAKAGE ON UP/DOWNLOAD, INTRACLOUD</td>
<td>Medium</td>
</tr>
<tr>
<td>Data are transferred more in transit and distributed across multiple physical machines.</td>
<td></td>
</tr>
<tr>
<td>INSECURE OR INEFFECTIVE DELETION OF DATA</td>
<td>Medium</td>
</tr>
<tr>
<td>Request to delete a cloud resource is made, this may not result in true wiping of the data.</td>
<td></td>
</tr>
<tr>
<td>DISTRIBUTED DENIAL OF SERVICE (DDOS)</td>
<td>Medium</td>
</tr>
<tr>
<td>DDoS to other user of cloud provider may impact</td>
<td></td>
</tr>
<tr>
<td>ECONOMIC DENIAL OF SERVICE (EDOS)</td>
<td>Medium</td>
</tr>
<tr>
<td>EDoS destroys economic resources; the worst case scenario would be the bankruptcy of the customer or a serious economic impact.</td>
<td></td>
</tr>
</tbody>
</table>

Technical risks are similar to Japanese users and EU users.

Survey Result
### Technical Risk 3

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOSS OF ENCRYPTION KEYS</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Disclosure of secret keys or passwords to malicious parties may impact to loss or leakage of important data</td>
<td></td>
</tr>
<tr>
<td><strong>UNDERTAKING MALICIOUS PROBES OR SCANS</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Malicious probes or scanning are indirect threats to the assets.</td>
<td></td>
</tr>
<tr>
<td><strong>COMPROMISE SERVICE ENGINE</strong></td>
<td>Medium</td>
</tr>
<tr>
<td>Provider service engine have vulnerabilities and is prone to attacks or unexpected failure.</td>
<td></td>
</tr>
<tr>
<td><strong>CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT</strong></td>
<td>Low</td>
</tr>
<tr>
<td>Hypervisor, or service engine may have vulnerabilities and is prone to attacks or unexpected failure.</td>
<td></td>
</tr>
</tbody>
</table>

Technical risks are similar to Japanese users and EU users.
### Legal Risk 1

<table>
<thead>
<tr>
<th>リスク</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBPOENA AND E-DISCOVERY</td>
<td>High</td>
</tr>
<tr>
<td>As a result of subpoena, storage as well as shared hardware is at risk of the disclosure to unwanted parties</td>
<td></td>
</tr>
<tr>
<td>User is not able to protect or preserve of evidence in the cloud when requested from Authorities</td>
<td>High</td>
</tr>
<tr>
<td>RISK FROM CHANGES OF JURISDICTION</td>
<td>High</td>
</tr>
<tr>
<td>User data may be held in multiple jurisdictions, some of which may be high risk</td>
<td></td>
</tr>
<tr>
<td>LICENSING RISKS</td>
<td>Medium</td>
</tr>
<tr>
<td>Licensing conditions and online licensing checks may become unworkable in a cloud environment.</td>
<td></td>
</tr>
</tbody>
</table>

EU organisations feels more legal risk than Japanese organisations.
3 Comparison with ENISA result (4)

Common Risk 1

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETWORK BREAKS</td>
<td>Medium</td>
</tr>
<tr>
<td>Potentially thousands of customers are affected at the same time.</td>
<td></td>
</tr>
<tr>
<td>NETWORK MANAGEMENT</td>
<td>High</td>
</tr>
<tr>
<td>Provider network may not be managed properly and capacity and connection failure may impact to users.</td>
<td></td>
</tr>
<tr>
<td>MODIFYING NETWORK TRAFFIC</td>
<td>Medium</td>
</tr>
<tr>
<td>Network traffic between user and provider may not be modified in case of network failure.</td>
<td></td>
</tr>
<tr>
<td>PRIVILEGE ESCALATION</td>
<td>Medium</td>
</tr>
<tr>
<td>Potentially root authority has been seizure and data may be disclosed or modified.</td>
<td></td>
</tr>
</tbody>
</table>

Japanese organisations are not seriously consider network issues. This is because Japanese telecom operator provide excessive quality services.

Survey Result

[Survey result chart with bars for critical, medium, small, and No categories]
### Common Risk 2

<table>
<thead>
<tr>
<th>Risk</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCIAL ENGINEERING ATTACKS</td>
<td>Medium</td>
</tr>
<tr>
<td>Provider may be attacked “social engineering” and may disclose user data or information.</td>
<td></td>
</tr>
<tr>
<td>LOSS OR COMPROMISE OF OPERATIONAL LOGS</td>
<td>Low</td>
</tr>
<tr>
<td>Provider may lose or compromise user logging data.</td>
<td></td>
</tr>
<tr>
<td>LOSS OR COMPROMISE OF SECURITY LOGS</td>
<td>Low</td>
</tr>
<tr>
<td>Provider may lose or compromise security logs.</td>
<td></td>
</tr>
<tr>
<td>BACKUPS LOST, STOLEN</td>
<td>Medium</td>
</tr>
<tr>
<td>Provider may lose or compromise backed up files.</td>
<td></td>
</tr>
</tbody>
</table>

Common risks are regarded less for Japanese users than EU users.
3 Comparison with ENISA result (4)

Common Risk 3

<table>
<thead>
<tr>
<th>リスク</th>
<th>ENISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNAUTHORIZED ACCESS TO PREMISES</td>
<td>Low</td>
</tr>
<tr>
<td>Provider facilities may be invaded and infrastructures may be compromised.</td>
<td></td>
</tr>
<tr>
<td>THEFT OF COMPUTER EQUIPMENT</td>
<td>Low</td>
</tr>
<tr>
<td>Provider equipment (storage) may be stolen and user data may be compromised.</td>
<td></td>
</tr>
<tr>
<td>NATURAL DISASTERS</td>
<td>Low</td>
</tr>
<tr>
<td>Provider may not continue providing services due to natural disasters (flood, earthquake, volcano, etc).</td>
<td></td>
</tr>
</tbody>
</table>

Japanese organisations are exposed more natural distress than EU organisations, but do not evaluate high risk.
4 Conclusion

• Anxiety for cloud computing
  • Many issues are similar and common among Japan and EU organisations.
  • Japanese organisations seek quality of services (non stop, guarantied) to cloud provider.
  • European organisations utilize cloud computing with quality for money.
  • European organisations feel higher risk on legal, lock-in, and loss of governance than Japanese organisations.

• Expectation to cloud computing
  • Japanese organization should regard cloud computing as the new service category lower quality in good price.
This Study is Supported by ITGI-Japan

Contact:
Yonosuke Harada, Professor Institute of Information Security,
E-mail: Yo-harada@iisec.ac.jp