Information Security Governance in Japan

September 6, 2005

TAKASHI ISHITOBI
Assistant Director, Office of IT Security Policy
Ministry of Economy, Trade and Industry
JAPAN

Information Security as a Management Task

- IT is increasingly influential on society, customers, management, and so on.
- "IT System Risk" is considered as an important risk factor by companies.
- So, it is necessary for "Information Security" to be recognized as a management task.

Q. What kinds of “risk factors” do you need to survey and analyze in future?

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Number of Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Risk</td>
<td>127</td>
</tr>
<tr>
<td>Credit Risk</td>
<td>119</td>
</tr>
<tr>
<td>Financial Risk</td>
<td>77</td>
</tr>
<tr>
<td>Real Estate Risk</td>
<td>57</td>
</tr>
<tr>
<td>Natural Disaster Risk</td>
<td>52</td>
</tr>
<tr>
<td>Human Factor Risk</td>
<td>64</td>
</tr>
<tr>
<td>Institutional Risk</td>
<td>75</td>
</tr>
<tr>
<td>IT System Risk</td>
<td>81</td>
</tr>
<tr>
<td>Business Risk</td>
<td>63</td>
</tr>
<tr>
<td>Technology Risk</td>
<td>52</td>
</tr>
<tr>
<td>Regulatory Risk</td>
<td>63</td>
</tr>
</tbody>
</table>

### Obstacles to Information Security Investments

Major reasons for the lack of progress by Japanese companies in information security measures have been identified by a survey, and include:

1. Inability to see cost effectiveness of investments (62.1%),
2. No indicated standards on how far measures should be taken (53.4%),
3. Too costly (51.5%).

<table>
<thead>
<tr>
<th>Obstacles</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Costs too much</td>
<td>51.5%</td>
</tr>
<tr>
<td>Unable to see cost effectiveness of investments</td>
<td>62.1%</td>
</tr>
<tr>
<td>Lack of sufficient training</td>
<td>39.6%</td>
</tr>
<tr>
<td>Too much of a burden on employees</td>
<td>19.6%</td>
</tr>
<tr>
<td>Insufficient know-how on developing measures</td>
<td>32.7%</td>
</tr>
<tr>
<td>No indicated standards on how far measures should be taken</td>
<td>53.4%</td>
</tr>
<tr>
<td>Unable to obtain the understanding of top management</td>
<td>14.4%</td>
</tr>
<tr>
<td>No custom of considering data as an asset</td>
<td>18.3%</td>
</tr>
<tr>
<td>No appropriate tools or services</td>
<td>13.6%</td>
</tr>
<tr>
<td>Other</td>
<td>0.3%</td>
</tr>
<tr>
<td>Did not answer</td>
<td>1.9%</td>
</tr>
</tbody>
</table>


### Need for Information Security Governance

#### Companies’ Responsibilities

Companies should ensure that information security measures are implemented proactively in a manner that takes into consideration the perspective of Corporate Social Responsibility (CSR) as a member of the IT society.

#### Government’s Roles

- The roles that government should take are:
  1. To establish an environment where companies’ efforts to ensure information security are directly connected to their appropriate evaluation, and
  2. to support the establishment of an environment encouraging voluntary efforts by companies to establish information security measures.

In order to fulfill their responsibilities as members of the IT society, companies should develop and implement continuously from the perspective of information security:

1. Corporate governance which takes CSR into consideration, and
2. A mechanism of internal control which supports it.

This means no less than incorporating the new concept of **"Information Security Governance"** into business management.
Establish “Information Security Governance”

Problems hindering companies’ efforts

1. It is difficult to make appropriate investments in information security because the risk that an IT incident will occur is unclear.
2. Existing measures and efforts toward information security are not directly linked to corporate value.
3. The need to ensure business continuity is not fully understood.

Tools for establishing “information security governance”

1. Information Security Measure Benchmark
   - Improving awareness of the management level through self-check process
   - “Gateway” to future assessment/certification by third party
2. Model of Information Security Reports
   - Promotes fair evaluation by stakeholders
   - Provides motivation for assessments/certification by third parties
3. Guideline for Business Continuity Plan
   - Realize importance of business continuity
   - Promote development of BCP

Basic Relationship between the 3 Tools
Establishment of security policy and/or internal rules
Access controls
Installation of anti-virus software tools
Implementation of information security audits and third-party certification
Internal training
Inspection of outsourcees
Preparation of business continuity plan
Physical security controls
Preparation of business continuity plan
Internal training
Inspection of outsourcees
Preparation of business continuity plan
Physical security controls

Desired Level
Current Security Level of Responding Company
Provides answers on the Web

Assessment Items (47 items Total)
Security Measures (25 items)
- Organizational efforts
- Physical/environmental measures
- Operations management of communications/network
- Development/maintenance and access control
- Status of incident countermeasures
Corporate Profile (15 items)
- Vulnerability of Business Structure
- Social impact

Desired Level
Survey results
Recommended actions

Companies categorized based on its company profile
Companies for which a high level of security is required
Desired Level (High)
Recommended actions
Desired Level (Medium)
Recommended actions
Desired Level (Low)
Recommended actions

Desired level set in accordance with the company category

Presentation of total score and recommended actions

Information Security Measure Benchmark (i)

Information Security Measure Benchmark (ii)

- The management class can ascertain the difference between the company's current condition and the desired level, and gain a clearer understanding of their goals with regard to information security.
- The core company of the group can use this Benchmark as common criteria for ascertaining the level of each company within the entire group so as to verify that a certain level of information security is being ensured within the group.
- When B-to-B transactions are executed, it will be possible to receive the results of a self-check based on this Benchmark from the counterpart company in order to verify the information security level of that company.

- Conducted a survey to approximately 6,000 companies, and 1,633 companies responded to the survey. Of the 1,633 respondents, 885 answered all questions.
- Desired level is above the average score, which is the top 1/3 of each category based on the results.
- These respondents were grouped into one of 3 categories (High/Med/Low).
### Model of Information Security Report (i)

- Through disclosing information on companies’ efforts toward ensuring information security, which is of high interest to society, their efforts are fairly evaluated by customers, investors, and other stakeholders.
- It is necessary to avoid placing an excessive burden on companies.

#### Basic Structure of Information Security Reports

<table>
<thead>
<tr>
<th>(i) Basic information</th>
<th>(iv) Planning and objectives of information security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Objective of issuing the report</td>
<td>• Action plan</td>
</tr>
<tr>
<td>• Precautionary statement</td>
<td>• Numerical targets (total score of “Information Security Measure Benchmark, etc.”)</td>
</tr>
<tr>
<td>• Period covered</td>
<td></td>
</tr>
<tr>
<td>• Department responsible, etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(ii) Management’s philosophy regarding information security</th>
<th>(v) Results and assessment of information security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Company’s policy on efforts concerning information security</td>
<td>• Results of plans</td>
</tr>
<tr>
<td>• Scope of coverage</td>
<td>• Assessments</td>
</tr>
<tr>
<td>• Position of stakeholders in the report</td>
<td>• Incident reports, etc.</td>
</tr>
<tr>
<td>• Message to stakeholders, etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(iii) Information security governance</th>
<th>(vi) Major area of focus of information security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information security management system (location of responsibility, organizational structure, compliance, etc.)</td>
<td>• Efforts that the company wants to emphasize such as personal information protection or its business continuity plan, etc.</td>
</tr>
<tr>
<td>• Risks concerning information security</td>
<td></td>
</tr>
<tr>
<td>• Information security strategy, etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(vii) Third-party assessment/certification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• ISMS Conformity Assessment Scheme</td>
<td>• ISMS Conformity Assessment Scheme</td>
</tr>
<tr>
<td>• Information Security Audit</td>
<td>• Privacy Mark System, etc.</td>
</tr>
</tbody>
</table>

### Model of Information Security Reports (ii)

#### Benefits for the Report Issuer

- **Fulfillment of Accountability**
  - Explain externally that IT-related risk affecting business is low

- **Generating New Added Value in Business**
  - Reflected in business strategy
  - Establishing brand name

#### Benefits for Stakeholders

- **Customers/Consumers**
  - Purchasing Decisions
  - Ascertaining the reliability of business counterparts

- **Business Counterparts**
  - Ascertaining the reliability of business counterparts

- **Investors and Analysts**
  - Assessment of possible investments

- **Rating Agencies**
  - Better analysis material

- **Employees**
  - Increased awareness and understanding of information security

---

Select report items and level of content based on company’s own circumstances.

[Minimum Items and Content Necessary]  [All Items and Content]
Guideline for Business Continuity Plan (i)

- Only about 10% of listed Japanese companies surveyed have prepared BCPs, while 47% of overseas companies have already prepared BCPs.
- About 70% of Japanese companies prepare BCPs as part of Corporate Governance or Corporate Social Responsibility (CSR), while half of overseas companies do so at the request of existing or prospective customers. Also, BCPs are a standard for selecting business counterparts overseas.

Guideline for Business Continuity Plan (ii)

- The Guidelines are designed to promote an understanding of the Business Continuity Plan (BCP) at companies that are considering developing such plans.
- They explain specific steps for developing a BCP from the basic concept.
- Business is increasingly dependent on IT, so concrete plans are based on the assumption that an IT incident is bound to occur.
- The reference material and best practice examples should be useful for explanations within companies.
Rating of Information Security Reports by Third-Party Institutions
- In the future, it is expected that third-party institutions, such as assessment organizations, media, and non-profit organizations, will assess Information Security Reports using their own unique viewpoints and assessment tools, and then release the results of those assessments in the form of ratings.
- This should increase interest among stakeholders and, as a result, encourage companies issuing the reports to make even more information security efforts, in order to improve their ratings.

Use of the Information Security Measure Benchmark and other Tools in Government Procurements
- It is hoped that government institutions and the like will actively use the Information Security Measure Benchmark as an index for assessing the reliability of bidders in procurement projects.
- It can be expected that this kind of application to government procurements will not only encourage information security measures at bidding companies, but also have the positive effect of leading in the future to the application of the information security tools to orders between private businesses.

Application in Assessments for Non-Life Insurance and Rate Calculations
- It is hoped that the non-life insurance industry will use the Information Security Measure Benchmark to assess the status of information security efforts at companies that wish to obtain non-life insurance and adjust the non-life insurance premium rate based on the assessed level of information security.

To Permeate Information Security Governance

Our Goal ~ Toward to Build “Culture of Security”

It is our sincere hope that the concept of Information Security Governance will become pervasive not only at the corporate management level but also in society overall and, as a result, encourage IT usage within companies in a manner that ensures reliability in order to increase corporate competitiveness.

At the same time, we also fervently hope this concept will ensure that companies fulfill their social responsibilities as members of the IT society and that it will, in turn, contribute to the building of a “culture of security.”

9 Principles in the "Guideline for the Security of Information Systems and Networks: Towards a Culture of Security" (July 2002)

2) Responsibility
“All participants are responsible for the security of information systems and networks.”
Thank you!

Contact Info: Takashi Ishitobi
ishitobi-takashi@meti.go.jp
TEL: +81-3-3501-0397
FAX: +81-3-3501-6639