Plan for Developing and Applying “Multi – Risk Communicator (MRC)”
- Support Tool for Risk Communication under Multiple Risk Environment -

29th September, 2004
School of Engineering, Tokyo Denki University
Professor
Ryoichi Sasaki
sasaki@im.dendai.ac.jp
Necessity of Multi – Risk Communicator (MRC)
Various Risks in Corporate Management

- **Primary Risk**: The risk taken positively in order to gain profits
- **Secondary Risk**: Information Security Risk, Personal Information Leakage Risk, Compliance Risk, Tax Risk etc.
- **Original Risk**: The risk at which reputation gets worse
Trend

Among them, **Information security risk** and **privacy risk** which contains personal information leakage risk becomes very serious.

<Examples>
(1) In August 2003, the Japan Post was infected with Welch caused by the mistake of NEC field engineer. The Japan Post required NEC reparation for damages.

(2) In February 2004, personal information of 4.6 million people leaked from Soft Bank BB. This Japanese company must have used more than 4 billion yen for first action against this issue. In addition, law suite of this issue was started.
The Feature of the Risk in a Corporate

1. Opposing Various Risks
2. Required Various Measures to each Risk
3. Many Participants
Security and Privacy

Concepts

Security
(Confidentiality, Integrity, Availability etc.)

Privacy
Protection of personal information

Measures

Security countermeasures
Intrusion prevention
Data secrecy etc.

Privacy countermeasure
Personal information leakage prevention
Anonymity maintenance

Compatibility? Conflict?

Technology

Security technology
Cryptography
Digital signature
Access control etc.

Privacy Technology
Anonymous channel, P3P
Ring Signature etc.
## Relation between the measure for security and privacy

<table>
<thead>
<tr>
<th>No</th>
<th>relation</th>
<th>example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>classificatio</td>
<td>explanation</td>
</tr>
<tr>
<td>1</td>
<td>Compatibility</td>
<td>The security measure is the means of protection of personal information.</td>
</tr>
</tbody>
</table>
| 2  | Conflict | If measure for security or privacy is adopted, formation of another side is difficult. | (a) Protection of personal information makes pursuit of intruder difficult.  
(b) Allowing an encrypted mail overlooks the spill of personal information.  
(c) Personal information is known from the data on a public key certificate. |
The Image of the Solution to the Conflict Concept

<Professional>

Solution by technology

<example>

Use of an attribute certificate etc.

<Decision-maker>

citizen etc.

○ declaration to select preference

The necessity for Multi - Risk Communicator (MRC)
The Feature of the Risk in a Company

1. Opposing Various Risks
2. Required Various Measures to each Risk
3. Many Participants
Various measure candidates against an information leakage

<table>
<thead>
<tr>
<th>Technical Measure</th>
<th>System Specification</th>
<th>Personal Information</th>
<th>Human Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access restrictions</td>
<td></td>
<td></td>
<td>Firm password</td>
</tr>
<tr>
<td>Extraction of a log</td>
<td></td>
<td></td>
<td>Thoroughness of a clear screen</td>
</tr>
<tr>
<td>Monitoring Cryptography</td>
<td></td>
<td></td>
<td>Display of a privacy policy</td>
</tr>
<tr>
<td>Anti-virus</td>
<td></td>
<td></td>
<td>Examination for the adoption</td>
</tr>
<tr>
<td>Storage of a backup file</td>
<td></td>
<td></td>
<td>Ethics education</td>
</tr>
<tr>
<td>Inhibition to write to external media</td>
<td></td>
<td></td>
<td>Procedure at the time of retirement</td>
</tr>
<tr>
<td>Scrapping the recording media at the time of destruction</td>
<td></td>
<td></td>
<td>Management of entering and leaving restriction of personal-belongings carrying in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ban on carrying in of recording media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Management of disposal garbage</td>
</tr>
</tbody>
</table>

Privacy policy, Chief Privacy Officer

Fumiaki YAMAZAKI「An information security and protection of personal information Full measure」 Nikkei Business Publication, Inc. 2003 It creates based on figure 1-4.
The feature of the Risk in a Company

1. Opposing Various Risks
2. Required Various Measures to each Risk.
   - The system to search for the optimal combination of measures is required.
3. Many Participants
The Feature of the Risk in a Company

1. Opposing Various Risks
2. Required Various Measures to each Risk.
3. Many Participants
   (1) business manager
   (2) citizens, consumers
   (3) mass media
   (4) employees

Importance of Risk Communication
The National Research Council (NRC) defines risk communication as "an interactive process of exchange of information and opinion among individuals, groups, and institutions." The definition includes "discussion about risk types and levels and about methods for managing risks."
Specifically, this process is defined by levels of involvement in decisions, actions, or policies aimed at managing or controlling health or environmental risks.

http://odphp.osophs.dhhs.gov/pubs/prevrpt/Archives/95fm1.htm
Definition of Risk Treated in each Learning Field

1) Economics etc.
   probability of loss arising

2) Sociology etc.
   elementary event which inflicts harm on individual lives and health, such as an accident and a calamity

3) Engineering etc.
   the product of the occurring probability $P$ of an un-safe event and magnitude of damage $M$
   $$R = P \times M$$

The definition in engineering is adopted.
The Present State of Risk communication

business
manager

mass
media

citizens
consumers

employees

All are insufficient.

A Risk Communication Support Tool is Required.
The reasons to develop MRC

1. A means to avoid confrontation of many risks is required.

2. The system which searches for the optimal combination of a measure is required.

3. A risk communication support tool is required.

Development of Multi-Risk Communicator
(Research Institute of Science and Technology for Society as Mission-oriented Research Program II Research on ‘Investigating means of reducing the vulnerability of highly sophisticated information society’)

Image of Multi – Risk Communicator (MRC)
Outline of MRC

Multি–Risk Communicator (MRC)

(6) Display for Participants

(5) Simulator (Continuous, Discrete)

(2) Total Controller

(4) Optimization Engine

(3) Formulation Supporter

Negotiation Infrastructure

Participants for decision making

(1) Display for Specialists

Specialist
1. Specialists decide (a) objective function (b) constraint functions (c) proposed measures (d) coefficient value (e) constraint values, in order to formulate as optimization problem.
Formulation Image as Binary Optimization Problem

Minimize Social Total Cost \( (x_i \mid i=1,2, n) \)

s.t. \( P(x_i \mid i=1,2, n) \leq P_t \)

\( S(x_i \mid i=1,2, n) \leq St \)

\( C_k(x_i \mid i=1,2, n) \leq C_{kt} (k=1,2, \ldots, K) \)

\( x_i = 1 \) or \( 0 \)

\( X_i : i \) th countermeasure

\( S : \) Function for Security Risk

\( P : \) Function for Privacy Risk

\( C_k : \) Function for Cost for participant \( k \)

To obtain these function, event tree analysis, fault tree analysis etc. is used
### Example of Analysis by the ETA

<table>
<thead>
<tr>
<th>Initial event</th>
<th>countermeasure</th>
<th>Sequence</th>
<th>event probability</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-key cryptography compromisation information check</td>
<td>correspondence policy enforcement at the time of compromisation</td>
<td>S1</td>
<td>( P1 = P0(1 - Pa) )</td>
<td>no injustice</td>
</tr>
<tr>
<td></td>
<td>securement of proof of user signature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>securement of proof of CA certificate</td>
<td>S2</td>
<td>( P2 = P0Pa(1 - Pb)(1 - Pc) )</td>
<td>no injustice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( P0 )</td>
<td>success (1 - Pa)</td>
<td>S3</td>
<td>( P3 = P0Pa(1 - Pb)Pc )</td>
<td>forgery and alteration are possible.</td>
</tr>
<tr>
<td></td>
<td>failure Pa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>success (1 - Pb) success (1 - Pc)</td>
<td>S4</td>
<td>( P4 = P0PaPb(1 - Pc) )</td>
<td>alteration is possible</td>
</tr>
<tr>
<td></td>
<td>failure Pb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>failure Pb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>failure Pc</td>
<td>S5</td>
<td>( P5 = P0PaPbPc )</td>
<td>forgery and alteration are possible</td>
</tr>
</tbody>
</table>

\[
\text{probability of alteration} = P3 + P4 + P5, \quad \text{probability of forgery} = P3 + P5^{21}
\]
Example of Modeling by FTA

- **get illegal contents**
  - get physically
    - get by copy physically
      - CD burning
        - intention of unjust acquisition
          - copy is possible
            - intention to copy
        - intention to circulate
      - intrusion to sever
  - get by theft
  - get electronically
    - get illegal access
      - get on communication path
        - intention of unjust acquisition
          - get Encryption contents
            - decryption is possible
              - get decryption key
              - code breaking
        - get by spoofing
      - use P2P
      - use HP
How to use MRC (2)

2. To obtain optimal combination of proposed measures, optimization engine is used. As result example, the measure 1, 3, and 6 is adopted as the optimal combination.
   
   (a) Brute force method
   (b) Branch and bound method
   (c) Implicit enumeration method etc.

Participants for decision making

Specialists
How to use MRC (3)

3. This result is displayed intelligibly for a participants using a simulator and the display for participants for risk communication.
Example of Modeling for Simulation Using System Dynamics

Image of Output

Value

Time
How to use MRC (4)

4. Each participant says the opinion “We propose to change the value of constraint” or “change coefficient value”, “adding a measure we propose” etc.

5. Formulation is changed by specialists
Muliti - Risk Communicator

For New Item

Input the name of New Item

Selection of Functions

1. Modeling
2. Formulation
3. Optimization Engine
4. Simulator
5. Interactive Display
6. Others
Image of Display for Specialists (3)

**Multi - Risk Communicator**

**Modeling Support**

1. Event Tree Analysis (ETA) Support
2. Fault Tree Analysis (FTA) Support
3. Others

**Other Displays**

Support for Formulation
Select the Method for Optimization
Select the Method for Simulation etc.
Risk Communication Process for participants

(1) Optimal Solution
(2) Formulated results
   (a) constraints
   (b) Variables etc

New values of constraint
New values of variables etc.

Negotiation Infrastructure

This process will be continued until satisfactory solution can be obtained.
Plan for Approach
Interactive Approach of Development and Application

Development of MRC

<Procedure>
Consider the function
Develop prototype
Modify

Computer Support Tool
Guideline

Representative Applications

Pilot Applying

Three or Four Typical Applications

Know How
Application candidate

Technology Oriented

Communication Oriented

(candidate)

1. Optimization of the measures against public-key cryptography compromise

2. Illegal copy prevention measures

3. The measure against a personal information leakage

4. Optimization of the measure under the environment where security and protection of personal information are opposed to each other (the resident registry network issue etc.)
The development item for prototype in fiscal 2004-2005

< fiscal 2004 >
1. Development of formulation support part (minimum)
2. Development of optimization engine part (minimum)
3. Integration of simulator
4. Display part (minimum)

< fiscal 2005 >
1. Brush up of the part in fiscal 2004
2. Construction of example database
3. Development of the MRC use interface for a participants check
4. Development of the MRC interface for a specialist check
Structure of Multi-Risk Communicator WG

WG committee

(A meeting will be held for deed orientation and advice about 10 times the fiscal 2004.)

University
- Murayama professor Iwate Prefecture University
- Yashima professor Tokyo Denki University
- Yoshiura associate professor The University of Electro-Communications

Company
- Maki NTT Data Corporation
  - Murase Mitsubishi Research Institute, Inc.
  - Sudo Oki Electric Industry Co., Ltd.
  - Hongo NTT DoCoMo Inc.

Research Group
- Tomoko Ohi full-time research worker
- Shinji Yamane part-time research worker
- Ishii, Ueda, Ohmomo Tokyo Denki University graduate students
Items to be solved

1. How to show the results to participants who do not have special knowledge?

2. How to treat when there is the participant who never satisfy?

3. etc
Schedule of research

Conflict of opinion

Basic Resident Registry Network
The measure against a personal information leakage
Illegal copy preventive measures
The measure against public-key cryptography compromisation

large

None

small

the experiment by the roll player
Treatment of a participation person

fiscal 2003-2004
fiscal 2005
fiscal 2006

Illegal copy preventive measures