World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:2, No:9, 2008

Application of "Multiple Risk Communicator" to the Personal Information Leakage Problem

Mitsuhiro Taniyama, Yuu Hidaka, Masato Arai, Satoshi Kai, Hiromi Igawa, Hiroshi Yajima, and Ryoichi Sasaki

***Abstract*—**Along with the progress of our information society, various risks are becoming increasingly common, causing multiple social problems. For this reason, risk communications for establishing consensus among stakeholders who have different priorities have become important. However, it is not always easy for the decision makers to agree on measures to reduce risks based on opposing concepts, such as security, privacy and cost. Therefore, we previously developed and proposed the "Multiple Risk Communicator" (MRC) with the following functions: (1) modeling the support role of the risk specialist, (2) an optimization engine, and (3) displaying the computed results. In this paper, MRC program version 1.0 is applied to the personal information leakage problem. The application process and validation of the results are discussed.

***Keywords*—**Decision Making, Personal Information Leakage Problem, Risk Communication, Risk Management.

I. Introduction

ALONG with the progress of our information society, various risks have become increasingly common, causing multiple social problems. For example, with the increased convenience in information networks, computer viruses and unauthorized access have caused damage to personal and corporate accounts. Moreover, with the availability of digital data, infringement of copyrights, such as illegal copies of all types of data, have occurred.

In order to deal with these social problems, opposing factors such as security, privacy, convenience, and cost have to be considered. Consequently, there has been a growing interest in risk communications and the process of establishing a consensus among people directly and indirectly involved. However, it is not always easy for decision makers to agree on the optimal combination of measures that reduce some risks with consideration of other risks.

To alleviate this problem, we previously proposed the "Multiple Risk Communicator" (MRC), which supports risk analysis and risk communication in our information society [1][2]. In this paper, MRC program version 1.0 is applied to the personal information leakage problem in a simulated enterprise. Although previous papers described a summary of MRC system and MRC application process, it did not explain a practical application process of MRC. A practical application process of MRC is described in detail and the evaluation of MRC is discussed in this paper.

Mitsuhiro Taniyama is with Tokyo Denki University, Japan.(e-mail: 07gmi15@ms.dendai.ac.jp).

Yuu Hidaka is with IT DORAKU Research Lab, Ltd.(e-mail: y.hidaka@dorakuken.co.jp).

Masato Arai, Satoshi Kai, and Hiromi Igawa are with Hitachi, Ltd.(e-mail: {masato.arai.ez, satoshi.kai.nf, hiromi.igawa.rq}@hitachi.com).

Hiroshi Yajima and Ryoichi Sasaki. are with Tokyo Denki University and RISTEX of the Japan Science and Technology Agency.(e-mail: {yajima, sasaki}@im.dendai.ac.jp).

II. Application of MRC to Personal Information Leakage Problem

A. Overview of MRC

The concept of MRC was examined and MRC program version 1.0 was developed in a previous study [1][2]. MRC was applied to social problems such as illegal copying, internal control, and compromising of public key ciphers. The objective of the MRC program is to reduce risk with consideration of the following.

Requirement 1: There are various conflicting risks, and measures to reduce one or more must consider all risks.

Requirement 2: Various measures are required for individual risks. Resolving every problem with one measure is not possible, and features for determining the most appropriate combination of measures are essential.

Requirement 3: For decision making, the individuals involved (e.g., managers, citizens, customers, and employees) must be satisfied. Therefore, features for supporting risk communications among these individuals are essential.

Precious study of risk analysis which satisfies above all requirements was not conducted. For example, Japanese Standards Association published "Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security", which classifies the methodologies of risk analysis into four categories [3]. Additionally, Bruce Schneier, who is an internationally renowned security technologist and author, describes the methodologies of risk analysis on his book "Beyond Fear" [4]. However, these methodologies are not sufficient to satisfy above all requirements. Therefore, we considered establishing the methodology of risk analysis which satisfies above all requirements is essential.

An overview of the MRC program for satisfying these requirements is shown in Fig. 1.

The basic feature satisfying Requirement 1 and Requirement 2 is the Optimization Engine, which is (4) in Fig. 1. In the optimization engine, a brute force method and lexicographic enumeration method are used to obtain the solution [5]. In particular, a discrete optimization problem with various measures proposed as 0-1 variables (or a 0-1 programming problem) is used. To formulate the discrete optimization problem easily, the Assistant Tool for Specialists (6) contains the functions of analysis, formulation and parameter setting. In addition, the fault tree analysis method for the risk analysis [6] is supported in this tool.

The Assistant Tool for Participants (1) satisfies Requirement 3 for decision making. The optimal combinations of measures obtained from the Optimization Engine (4) enable decisions to be made more easily by the individuals involved. Opinions such as"Add the measures we propose" and "We propose to change the value of this constraint" are sent to the specialist via the Negotiation Infrastructure (5). Then, the facilitator supports the communication between the participants and the specialist.

The Total Controller (3) and Database (2) link the processing of these components.

The MRC program is implemented using Java and PHP 5.2 in a Windows XP environment. The total number of coding steps is approximately 10,000. Apache 2.24 is used for the Web server, MySQL 5.0 for the database server, and Xoops 2.0.16 for the communication server. In addition, Mathematica 5.2 is used by the specialist to calculate the numerical formulas in the PC.

The MRC application process is shown in Fig. 2. The Preparation Process and MRC Usage Process, shown in this figure, are described in Sections III and Section IV, respectively.

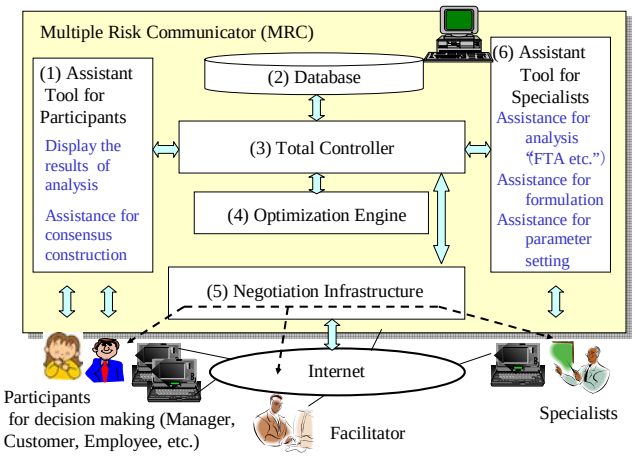

Fig. 1 Overview of MRC

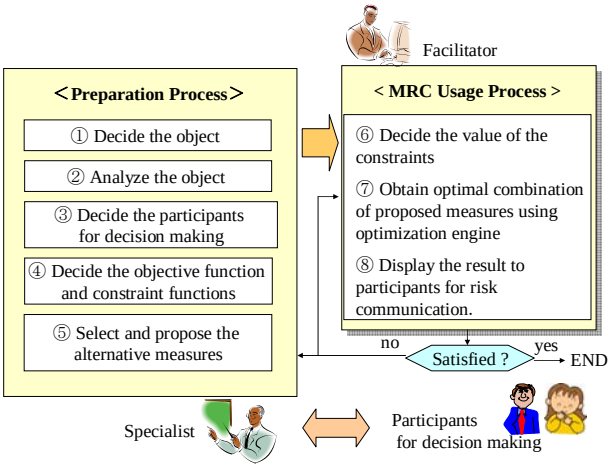

Fig. 2 MRC Application Process

B. Personal Information Leakage Problem

On several occasions in recent years, many organizations such as businesses and schools have accidentally leaked personal information, and such leakages have become a social problem in Japan. According to a report published by the Japan Network Security Association, 993 incidents occurred in 2006 [7]. If an organization leaks personal information, it loses the trust of the people. This sequence of events can potentially lead to a decreased number of customers and decreased stock price.

For this reason, many organizations have taken measures to avoid such a problem. Such measures, however, can lead to further problems. For example, employees in one enterprise may be dissatisfied with decreased convenience and privacy caused by applying strict measures. Meanwhile, the customers whose information is stored by the enterprise may not want their personal information to be leaked. Moreover, the executive officer in the enterprise would like to keep the cost as low as possible.

Given the above information, it is easy to understand the difficulties in applying measures that establish consensus among these stakeholders. Therefore, we decided to apply MRC to the personal information leakage problem.

III. Risk Analysis of the Personal Information Leakage Problem

A. The Enterprise Analyzed

Following the Preparation Process shown in Fig. 2, we consider a simulated enterprise whose sales department handles ten million pieces of personal information. The number of employees is approximately 1,820. Only 20 of these employees are allowed to go into the server room. However, employees who are not allowed to go into the server room can get personal information from the server as deemed necessary. After obtaining permission from the manager, the employees can receive a minimal amount of personal information.

B. Decision of the Objective and Constraint Functions

B.1 Objective Function

The objective function decides the combination of measures. Formulation of the objective function is described as follows.

Min {Total risk of information leakage + Total cost of measures}

where,

Total risk of information leakage = Value of one piece of personal information x the number of leaked personal information per incident x probability of leakage for a year. The Total cost of measures is calculated using the parameters seen in TABLE III.

The variables of the Total risk of information leakage equation are defined in more detail in the following.

(1) Value of one piece of personal information: For our simulated enterprise, this is defined as 10,000 Japanese Yen (The U.S. dollar traded at about 109 Japanese Yen, on August 27, 2008.) based on an incident in Uji City in Kyoto, Japan. One organization, accused of personal information leakage, was sentenced to pay 10,000 Japanese Yen for pain and suffering of the plaintiff.

(2) The number of leaked personal information per incident: This information was obtained from a report published by the Japan Network Security Association [7] [8] [9]. This report, which has been published every year since the year 2002, summarizes the investigation of articles about personal information leakage problems. The number of items of leaked personal information is classified and determined by the following sources of (a)–(d) seen below. In this risk analysis, the number of leaked personal information per incident was obtained as averaged data from 2004 to 2006 reports. It is supposed that the server in the computer room of the enterprise has ten million pieces of personal information. A summary of these leaked items is as follows.

(a) Leakage from the server: Ten million pieces of personal information

(b) Leakage from laptop or desktop computer: 4,734 pieces of personal information

(c) Leakage from portable devices, e.g., USB memory, hard disk, floppy disk, CD/DVD: 7,120 pieces of personal information

(d) Leakage from print: 537 pieces of personal information

(3) Probability of leakage for a year is obtained by using the fault tree analysis which is described in section D.

B.2 Constraint Functions

The constraint functions are decided as follows:

(1) Cost of measure for the executive officer

(2) Probability of leakage (for one year) for the customer

(3) Degree of burden on employee's convenience

(4) Degree of burden on employee's privacy

Formulations of each of these constraint functions are described as follows (in the order presented above):

$$(1)\ \sum_{i=1}^{n} Co_i X_i \le Co_t$$

$$(2)\ f_p(X_1, X_2, ..., X_n) \le P_t$$

$$(3)\ \sum_{i=1}^{n} E_i X_i \le E_t$$

$$(4)\ \sum_{i=1}^{n} \mathrm{Pr}_i X_i \le \mathrm{Pr}_t$$

Here, Xi, represented as 0-1 variables, is a flag indicating whether to take the measures; Coi, Ei, and Pri are calculated by the parameters of the measures; fp is represented as the probability of leakage for one year, and is calculated using the Fault Tree Analysis which is described in section D.

C. Selection of Measures

We decided the following prerequisites for the measures proposed (Table I).

TABLE I
PREREQUISITES FOR PROPOSED MEASURES

No	Detail
1	A firewall is installed.
2	Antivirus software and security patches are installed on all computers.
3	Employees cannot enter the server room without an identification card.
4	Employees are required to enter their password when they log into their PC.
5	Employees are required to put papers that contain personal information through the shredder.
6	Employees are required to get the manager's permission when they remove their laptop or USB memory from the enterprise.
7	Employees are permitted to take printed information out of the enterprise.

Because these measures are established by many enterprises according to the report of the Japan Network Security Association, these were selected not as measures but as prerequisites [10]. Considering the above prerequisites, we selected the following 15 measures (Table II).

The measures and the value of parameters were obtained by discussions among the employees in the enterprise (Table III). In the cases of 6 and 7, 8 and 9, and 10 and 11 from the proposed selection of measures chart, only one of the alternate details were selected. This is due to the similarity of the measures in each of the details. The cost was obtained by investigating product brochures. Although the cost is originally represented as Japanese Yen, it is transformed into the U.S. dollar because it is known all over the world. Exchange rate on August 27, 2008 (1 U.S. dollar: 109 Japanese Yen) was used. The degree of burden on an employee's convenience and privacy ranges from 0 (minimum) to 1.0 (maximum). If a satisfactory probability to decrease leakage is 0.8, the information leakage is decreased by 80% in an event of the fault tree. Although the value of the satisfactory probability is actually set with more specificity, some factors are omitted here due to limited space.

TABLE II
PROPOSED SELECTION OF MEASURES

No	Detail
1	Install a system to force employees to change their password four times a year.
2	Install management software to prohibit employees from using software that the manager does not allow.
3	Install management software to prohibit employees from using portable devices with the server.
4	Install a surveillance camera.
5	Install a URL filtering tool to prevent the use of web-based email and message-board postings.
6	Install a mail filtering tool to restrict emails sent and received. (Employees cannot send email out of the enterprise without sending a copy of the mail to the manager.)
7	Install a mail filtering tool to restrict emails sent and received. (Employees cannot send email only containing an attached file out of the enterprise without sending a copy of the mail to the manager.)
8	Install management software to encrypt the data automatically when employees try to copy data from a desktop or laptop computer to a portable device. (They cannot decode the data without a computer in the enterprise.)
9	Distribute USB memory which encrypts the data automatically to all employees.
10	Install a system to automatically encrypt the data stored in a laptop computer.
11	Distribute thin client computers to employees.
12	Restrict the taking of printed personal information out of the enterprise.
13	Install a system to automatically put watermarks on the print.
14	Install a intrusion detection system.
15	Install a security scanning system at all entries into the enterprise.

D. Fault Tree Analysis

Fault Tree Analysis (FTA) [6] was used to quantify the risk of the probability of personal information leakage. The process of FTA is described as follows.

(1) Define the undesired effect.

(2) Each event that could cause the top event is added to the tree as a series of logic expressions.

(3) The probabilities of the lowest event are obtained from the statistics or opinions of experts.

(4) The probability of the top event is obtained from the calculation of the events as defined in the previous steps (2)-(3).

Here, five Fault Trees were made. The top events of these were (1) Leakage from the server, (2) Leakage from a desktop PC, (3) Leakage from printed information, (4) Leakage from a laptop, and (5) Leakage from a portable device (e.g., USB memory, portable hard disk, CD/DVD). Lower events are (1) Leakage by the employees, (2) Leakage by an external person who has stolen from the enterprise, and (3) Leakage by an external person occurred when information was stolen outside of the enterprise. These lower events were also analyzed.

The probability of the lowest event was obtained using reports from the Japan Network Security Association [7] [8] [9].

IV. RISK COMMUNICATION USING THE MULTIPLE RISK COMMUNICATOR

This section describes the MRC Usage Process, presented in Fig. 2. The data obtained by the risk analysis was input into the MRC program. We conducted an experiment of risk communication to establish the consensus among role players, as follows.

Role player

(1) Executive officer : a professor at Tokyo Denki University

(2) Customer : a student at Tokyo Denki University

(3) Employees : two employees in the enterprise

TABLE III
PARAMETERS OF PROPOSED MEASURES

No.	Satisfactory probability to decrease leakage					Cost (U.S. $)	Convenience burden	Privacy burden
	Server	Desktop computer	Print	Laptop computer	Portable device			
1	0.8	0.8		0.5		167,823.12	0.8	0
2	0.65	0.65		0.85		164,766.06	0.5	0
3	0.99					770.64	0.4	0
4	0.4	0.4	0.2	0.4	0.4	38,532.11	0	0.5
5	0.7	0.7		0.7		89,339.45	0.4	0
6	0.8	0.8		0.8		51,880.73	0.6	0.6
7	0.75	0.75		0.75		67,431.19	0.4	0.5
8		0.99		0.99	0.999	265,967.89	0.2	0
9					0.999	330,275.23	0.3	0
10				0.999		140,256.88	0.3	0
11				0.999		2,642,752.29	0.4	0
12			0.8			198,165.14	0.7	0
13			0.6			397,506.88	0.1	0.1
14	0.75					179,541.28	0	0
15	0.8	0.8	0.8	0.8	0.8	22,935.78	0.3	0

(a) First, a specialist who has a skill to use the MRC program conducts the optimization using MRC if no measures have been adopted. The reason why we obtained the probability of leakage is to enable the participants to decide the value of constraints more easily. The results are shown in Table IV.

TABLE IV
CASE IN WHICH NO MEASURES ARE ADOPTED

Cost (U.S. $)	0
Probability of Leakage (for one year)	0.3036
Burden on Employee's Convenience	0
Burden on Employee's Privacy	0
Measures	
Optimal Value (U.S. $)	12,310,247.95

(b) Second, the specialist sets the value of the constraints, as shown in Table V, and conducts the optimization using MRC. In our experiment, the cost constraint was half of the cost (1,504,331.28 U.S. $) when considering all measures. The probability of leakage was half of the probability (0.1518) when no measure was adopted because of the customer's desire. Because there were some opinions from the stakeholders that were difficult for setting the value of the convenience and privacy burdens, we set these as the maximum values. Optimized solution A, shown in Table VI, was obtained for this constraint.

TABLE V
CONSTRAINT CONDITIONS

Cost (U.S. $)	1,504,331.28
Probability of Leakage (for one year)	0.1518
Burden on Employee's Convenience	4.5
Burden on Employee's Privacy	1.2

TABLE VI
OPTIMIZED SOLUTION A

Cost (U.S. $)	830,749.72
Probability of Leakage (for one year)	0.14328
Burden on Employee's Convenience	2.5
Burden on Employee's Privacy	0.6
Measures	1,2,3,6,8,14
Optimal Value (U.S. $)	1,664,448.57

(c) Third, optimized solution A was suggested to the stakeholders. After reviewing optimized solution A, the customers suggested further decreasing the probability of leakage. Accordingly, the probability of leakage was set as one-third of the probability (0.1012) when no measure was adopted. Then, we conducted the optimization again. However, no optimized solution was obtained.

For this reason, the customers again suggested setting the probability of leakage as two-fifths (0.12144). Optimized solution B, shown in Table VII, was obtained for this constraint.

TABLE VII
OPTIMIZED SOLUTION B

Cost (U.S. $)	1,169,171.74
Probability of Leakage (for one year)	0.12001
Burden on Employee's Convenience	3.5
Burden on Employee's Privacy	0.6
Measures	1,2,3,6,8,10,12,14
Optimal Value (U.S. $)	1,998,456.07

(d) Although customers were satisfied with optimized solution B, employees were dissatisfied because employees thought that strict measures were adopted and it would cause work inconvenience. Particularly, because the convenience burden of measure No. 6 (Employees cannot send email out of the enterprise without sending a copy of the mail to the manager) is very high, employees suggested not implementing No. 6. The customers and executive officer agreed with this demand and decided not to adopt No. 6.

However, since employees said that they could adopt No. 7 (Employees cannot send email containing an attached file out of the enterprise without sending a copy of the mail to the manager), they decided to adopt No. 7 instead of No. 6. Optimized solution C, shown in Table VIII, is obtained for this constraint.

TABLE VIII
OPTIMIZED SOLUTION C

Cost (U.S. $)	1,184,722.20
Probability of Leakage (for one year)	0.12439
Burden on Employee's Convenience	3.3
Burden on Employee's Privacy	0.5
Measures	1,2,3,7,8,10,12,14
Optimal Value (U.S. $)	2,015,937.31

(e) Although the probability of leakage slightly increased, customers were not dissatisfied with optimized solution C. Employees were satisfied by adopting No. 7 instead of No. 6. Although the cost of optimized solution C was more expensive than solutions A and B, the executive officer accepted it. Consequently, all participants were satisfied with optimized solution C, and they succeeded in establishing consensus.

V. EVALUATION OF THE MRC

A. Evaluation of Objective Function

As defined in this paper, the damage caused by one piece of personal information leakage was set at 10,000 Japanese Yen. However, to be exact, we should consider the damage caused by the decrease of trust in the enterprise and the decrease of the stock price. Moreover, the expenses incurred when dealing with mass media and lawyers must be considered. These are issues of risk analysis for future work.

B. Evaluation of the Constraint Function

When the stakeholders decided the value of the constraints, there was a general opinion that it is difficult to understand and decide the degree of burden on convenience and privacy. Hence, we let employees select which measures they did not want to take. As a result, the risk communications went

smoothly and we obtained knowledge for using this method that helps the stakeholders decide the constraint more easily.

C. Evaluation of Risk Communications

Because the experiment of risk communications was a simulation conducted by role players, they easily succeeded at establishing consensus. However, if the risk communication was conducted by actual stakeholders, it is thought that establishing consensus would become more difficult. In particular, although the executive officer did not complain about the cost in this risk communication, this agreement rarely happens with actual stakeholders.

In future work, we plan to conduct risk communications with actual stakeholders. We have developed the MRC program version 2.0, which supports risk communications in more varied ways [11]. We will to conduct risk communications with this new version.

D. Usefulness of the MRC

In this section, we describe the optimized combination of measures which was obtained by several experts who are very familiar with the personal information leakage problem. These measures were set in MRC, and the result is shown in Table IX.

TABLE IX
MEASURES OBTAINED BY EXPERTS' DISCUSSION

Cost (U.S. $)	970,235.96
Probability of Leakage (for one year)	0.13479
Burden on Employee's Convenience	2.4
Burden on Employee's Privacy	0.6
Measures	1,2,6,8,10,14
Optimal Value (U.S. $)	1,801,672.14

Consequently, the measures selected by the experts and the measures of optimized solution A obtained by the MRC are almost identical. However, the measures selected by the experts and the measures of optimized solution C, which established consensus finally among the simulation stakeholders, differed. Therefore, discussions among stakeholders and changes of the values of the constraints again and again using the MRC can lead to a combination of measures which satisfy all stakeholders. Furthermore, once we analyze the problem and put the data into the MRC program, we can use it as a template for different organizations. This will expedite the determination of optimized measures.

VI. CONCLUSION

MRC program version 1.0 was applied to the personal information leakage problem, and the results are described in this paper. Although the stakeholders used in the simulation were merely role players, not actual decision makers, they could establish consensus of the combination of measures using the MRC program. Thus, it can be concluded that MRC is useful for establishing consensus of decision makers in a multiple risks environment.

In future work, we will use MRC to consider the crisis management plan we should consider for personal information leaks.

ACKNOWLEDGMENT

The present research was sponsored by Mission Program 2, Clarification and Resolution of Vulnerabilities of an Advanced Information Society, of the Japan Science and Technology Agency's Research Institute of Science and Technology for Society.

REFERENCES

[1] Ryoichi Sasaki, Saneyuki Ishii, Yuu Hidaka, Hiroshi Yajima, Hiroshi Yoshiura, Yuuko Murayama, "Development Concept for and trial application of a "multiplex risk communicator", IFIP I3E2005, Springer.
[2] Ryoichi Sasaki, Yuu Hidaka, Takashi Moriya, Mitsuhiro Taniyama, Hiroshi Yajima, Kiyomi Yaegashi, Yasumasa Kawashima, Hiroshi Yoshiura, "Development and applications of a Multiple Risk Coomunicator", Risk Analysis 2008.
[3] Japanese Standards Association, "Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security", 2001.
[4] Bruce Schneier, Beyond Fear, Springer, 2006.
[5] R.S. Garfinkel et al.: Integer Programming, Wiley and Sons, 1972.
[6] N.J. McCormick: Reliability and Risk Analysis, Academic Press Inc., 1981.
[7] Japan Network Security Association, "2006 Information Security Incident Survey Report", http://www.jnsa.org/result/2006/pol/insident/070720/2006incidentsurvey-e_080403.pdf
[8] Japan Network Security Association, "2005 Information Security Incident Survey Report", http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf
[9] Japan Network Security Association, "2004 Information Security Incident Survey Report", http://www.jnsa.org/houkoku2004/incident_survey_en.pdf
[10] Japan Network Security Association, "Fiscal 2003 Information Security Incident Survey Report", http://www.jnsa.org/houkoku2003/incident_survey1_e.pdf
[11] Hiroshi Yajima, Tomohiro Watanabe, Ryoichi Sasaki, "Evaluation of the Participant-Support Method for Information Acquisition in the "Multiplex Risk Communicator", 12th International Conference on Human-Computer Interaction 2007.