2012 3rd International Conference on e-Education, e-Business, e-Management and e-Learning
IPEDR vol.27 (2012) © (2012) IACSIT Press, Singapore

Development and Application of "MRC-Lite" to Support Easily Multiple Risk Communication

Kenta Oishi[1], Takashi Shitamichi[1], Ryoichi Sasaki[1]

[1] Tokyo Denki University, 2-2 Kanda Nishiki-Cho, Chiyoda-Ku, Tokyo 101-8457 Japan

Abstract. When considering multiple risks and costs in risk communications with a few participants, it is not easy to agree on the most appropriate combination of countermeasures. To support risk communications, the "Multiple Risk Communicator" (MRC) was previously developed. However, the MRC requires expert knowledge to formulate the input and execute the program. In this paper, we describe the development of "MRC-Lite," which is an MS-Excel based program, to solve the problems of the original MRC. We also present the results of a trial application of the personal information leakage problem.

Keywords: IT Risk, Risk Analysis, Risk Communication

1. Introduction

Along with the progress of our information society, the misuse of information networks and digital information have caused various social problems. Examples of criminal or unethical misuse include unauthorized access, copyright infringement by illegal copying, and computer viruses that affect individuals and corporations. The damage due to these actions is extensive.

To deal with these problems, complicated factors must be considered. These factors include not only the risk to security and cost, but also the convenience of information networks. Managing risk effectively requires both risk analysis and risk communications between participants with direct or indirect relationships. Risk analysis considers the optimal combination of countermeasures, because only one countermeasure to define risk management is usually not sufficient. Communication reduces the misunderstandings and lack of understanding among the individuals involved.

It is not easy for decision makers to agree on the optimal combination of countermeasures in risk communications because of the multiple risks. Thus, we previously proposed the "Multiple Risk Communicator" (MRC), which supports risk analysis and risk communications in our information society. We developed the "MRC program" as a support tool [1][2]. However, the original MRC has many input fields, including constraint functions and coefficients, and consequently requires much preparation time before starting a risk communication. In addition, the MRC program must be used with a PC containing Mathematica 5.2, and the PC must be connected to the Internet to read and write data in an external DB. Furthermore, not everyone can use the MRC program because it requires expert knowledge to formulate the input for analysis and communication.

To solve the problems of the original MRC， we developed "MRC-Lite," which everyone can easily use, although the functions to obtain the optimized combination of countermeasures for all information problems have not been implemented. MRC-Lite has the following advantages: it finds the optimized solution in a short time, does not need Mathematica 5.2, does not have to be connected to the Internet, and does not need specialized knowledge for the formulations.

In this paper, we outline the original MRC first, then describe the proposed MRC-Lite. We also present the results of a trial application of the personal information leakage problem. To assess the risk in the form of easy-to-read lists, we implemented the risk analysis techniques of the ISO27000 series of information security standards [3] and evaluated the risk by using a matrix [4]. Our proposed system is unique in that it can quickly generate a combination of countermeasures for multiple risks for multiple participants. At this stage, however, we can only apply the system to the problem of personal information leakage.

2. Multiple Risk Communicator (MRC)

2.1. Overview of the MRC

The original MRC is a system that deals with various risks, communicates with participants on objective, obtains the combination of optimized countermeasures, and supports consensus formation. The MRC program consists of the following, as shown in Fig. 1: Assistant Tool for Participants, Database, Total Controller, Optimization Engine, Negotiation Infrastructure, and Assistant Tool for Specialists.

2.1.1. Assistant Tool for Participants

Assists participants in decision making and displaying the analysis result.

To formulate the discrete optimization problem easily, the Assistant Tool for Specialists contains the functions of analysis, formulation, and parameter setting.

2.1.2. Database

Maintains solutions and opinions with the capability to access them as necessary.

2.1.3. Total Controller

Controls the entire program.

2.1.4. Optimization Engine

Finds the optimized solution of countermeasures by a brute force method and a lexicographical enumeration method.

2.1.5. Negotiation Infrastructure

Once the participants enter their opinions, the opinions are sent to the specialists through the Negotiation Infrastructure and the results are displayed.

2.1.6. Assistant Tool for Specialists

Assists the specialists in the input of constraint functions, countermeasures, parameters and constraint values into the MRC.

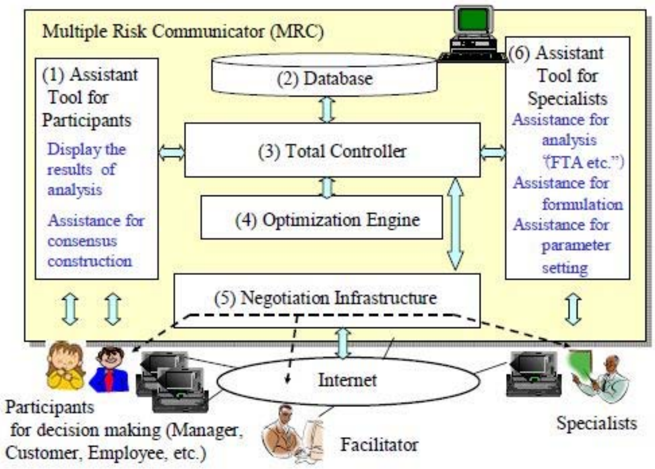

Multiple Risk Communicator (MRC)
(1) Assistant Tool for Participants
Display the results of analysis
Assistance for consensus construction
(2) Database
(3) Total Controller
(4) Optimization Engine
(5) Negotiation Infrastructure
(6) Assistant Tool for Specialists
Assistance for analysis (FTA etc.")
Assistance for formulation
Assistance for parameter setting
Internet
Participants for decision making (Manager, Customer, Employee, etc.)
Facilitator
Specialists

Fig. 1: Overview of the MRC

2.2. The MRC Procedure

The flow of the MRC application is described in the following.

2.2.1. Fix the objective problem

Fix the problem corresponding to the requirements from the participants who want to solve the problem.

2.2.2. Analyze the problem

Analyze the reason why the problem occurred and how the injustice was created, and determine the countermeasures.

2.2.3. Determine the participants for decision making

The specialist determines the participants who can address the problem.

2.2.4. Fix the objective function and the constraint function

The specialist determines the objective function and the constraint function. The objective function is a function to determine the combination of optimized countermeasures. The constraint function is a constraint to reflect the opinions of the participants.

2.2.5. Analyze the risk

To quantify a risk, the specialist performs a fault tree analysis (FTA) [5].

2.2.6. Determine the various countermeasures

The specialist determines the proposed countermeasures that are effective against the risk.

2.2.7. Input the results into the MRC program

The specialist inputs the results of the risk analysis into the MRC.

2.2.8. Determine the value of the constraint function

The facilitator, who has the role of leading and promoting the discussion, determines the values of the constraint function. The specialist inputs them into the MRC.

2.2.9. Show the results and obtain the consensus formation.

The MRC displays the results (optimized solution) to the participants. To reach a consensus on the combination of countermeasures, the participants engage in risk communications. If they are not satisfied with the optimized solution of the MRC, the specialist again runs the MRC program after changing the values of the constraint function and the proposed countermeasures. Until obtaining the consensus, the participants continue the risk communications.

2.3. MRC Application

To prove its effectiveness, the MRC was applied to solve the problems of personal information leakage and internal controls [2] [6]. However, the MRC needs much time to engage in risk communications due to the many inputs, such as the constraint functions and coefficients. In addition, Mathematica 5.2 must be installed into a PC that is connected to the Internet to read and write data in an external DB. Furthermore, it takes much time to perform the calculations to obtain the optimized solution. These requirements prevented some people from using the MRC. Therefore, a solution for those problems was required.

3. MRC-Lite

3.1. Overview of MRC-Lite

To solve the problems mentioned above, a function of software to support everyone who wants to easily carry out a risk communication was required for MRC-Lite. An overview of MRC-Lite is as follows.

3.1.1 Development environment

We developed MRC-Lite with MS-Excel so that users would not need a network. Many PC users install MS-Excel as software, and so users can presumably operate MRC-Lite. If a program is applied to solve all risk communication problems, it would be very complicated and enormous. Therefore, MRC-Lite deals only with the specialized topic of the personal information leakage problem. The development environment is Excel 2007, the language is VBA (Visual Basic for Applications) and the number of steps is approximately 1,300.

3.1.2 Method for the optimized solution

The original MRC calculates the optimized solution that meets the constraint function and makes the objective function maximal or minimal by applying a brute force method and a lexicographical enumeration method. These operations consume much time. As an example, when the MRC chose the optimized solution for the personal information leakage problem in a major company from 15 countermeasures, the PC (memory 1 GB，CPUCore (TM) Duo U2400 1.06 GHz) needed approximately ten minutes. Consequently, with MRC-Lite, we decided not to find the optimized solution and adopted countermeasures based on the value of the constraint function, in a cost-effective ranked order. In the example above, the precision of the selected countermeasures with MRC-Lite was lower than that with the MRC. However, it took MRC-Lite only two seconds to choose one of the 15 countermeasures; so, MRC-Lite obtained the optimized solution in much less time than that needed for the MRC.

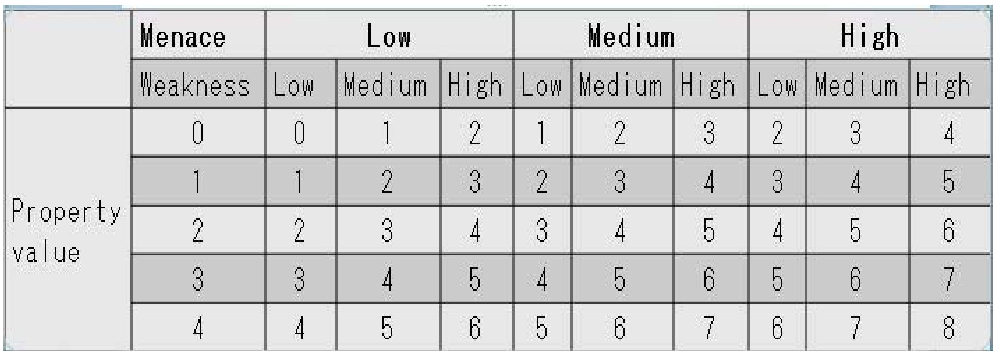
3.1.3 Comparison function of the optimized solution in the consensus formation process

For various applications of the original MRC, the comparison function of the optimized solution is given in the process of consensus formation. The comparison function is necessary for better risk communication. Consequently, MRC-Lite has functions to obtain logs for the optimized solution and compare them for better risk communications.

3.1.4 Risk analysis technique

The MRC performs an FTA to quantify a risk, but the FTA takes much time, as stated previously. Therefore, MRC-Lite uses the risk analysis technique of the ISO27000 series of information security standards [3], which uses an analysis with a precision lower than that of the FTA but can analyze a risk in a short time. The analysis method determines a risk qualitatively with nine phases from 0 to 8 in the three perspectives of property value, menace, and weakness (Table 1). As mentioned above, MRC-Lite does not support performing an FTA itself but will accept the input of the results of a risk analysis using FTA.

Table 1: Risk analysis technique of the ISO27000 series



	Menace	Low			Medium			High		
	Weakness	Low	Medium	High	Low	Medium	High	Low	Medium	High
Property value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

3.2. MRC-Lite Operation Method

The procedure of MRC-Lite is presented below.

3.2.1 Determine the input for the proposed countermeasures

Determine the input for the effective proposed countermeasures and the cost.

3.2.2 Determine the input for the effectiveness value of the proposed countermeasures

Determine qualitatively the effectiveness value of every proposed countermeasure by using the ten phases from 0 to 9. In the case of the effectiveness of the proposed countermeasure for the personal information leakage problem, it is assumed that 9 is the most effective and 0 is not effective. Then, as previously mentioned, the risk, determined qualitatively with the nine phases from 0 to 8 according to the three perspectives of property value, menace and weakness, is input with the weighting of the risk. Then, a risk analysis with methods such as the risk analysis technique of the ISO27000 series is performed to determine the risk qualitatively.

3.2.3 Determine the derivative risk

The derivative risk is the constraint function that is qualitatively determined with ten phases from 0 to 9. The burden on the employee's convenience (the numerical value of the business efficiency that drops by increasing the countermeasures) and the burden on the employee's privacy (the numerical value of the infringed privacy that increases by increasing the countermeasures) are set as the derivative risk, which is discussed and determined by every countermeasure. The degree of burden is shown in Table 2.

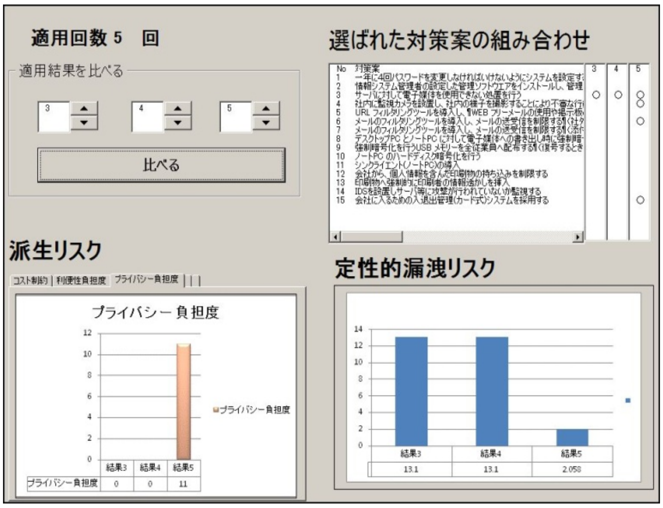
3.2.4 Input the values of the constraint functions

Input the cost and the constraint values of the derivative risk. If necessary, the function of screening the results is configured. If this function is adopted, “O” is input. If not adopted, "X" is input.

3.2.5 Show the optimized solution

The adopted proposed countermeasures, cost, derivative risk, qualitative leak risk (index of how much the risk is restricted) are shown to the participants. To form a consensus for the combination of countermeasures of the optimized solution brought by MRC-Lite, risk communications are held among the participants. If a participant is not satisfied with the optimized solution of the MRC-Lite, the constraint values and/or proposed countermeasures are changed, and the risk communications are continued until a consensus of the combination of countermeasures is reached.

An example of a screen shot of the optimized solution is shown in Fig. 2. In the top left corner of the figure, the number of executions of the application is shown. In addition, the adopted countermeasures can be compared. In the top right corner of the figure, a combination of the selected proposed countermeasures is shown. In the bottom of the figure, the derivative risk and the qualitative leak risk are shown clearly and visually with graphs.



No	対策案	3	4	5
1	一年に4回パスワードを変更しなければいけないようにシステムを設定す			
2	情報システム管理者の設定した管理ソフトウエアをインストールし、管理			
3	サーバに対して電子媒体を使用できない処置を行う	○	○	○
4	社内に監視カメラを設置し、社内の様子を撮影することにより不審な行			○
5	URL フィルタリングツールを導入し、¶WEB フリーメールの使用や掲示板			
6	メールのフィルタリングツールを導入し、メールの送受信を制限する¶(社			○
7	メールのフィルタリングツールを導入し、メールの送受信を制限する¶(添			
8	デスクトップPC とノートPC に対して電子媒体への書き出し時に強制暗			
9	強制暗号化を行うUSB メモリーを全従業員へ配布する¶(復号するとき			
10	ノートPC のハードディスク暗号化を行う			
11	シンクライエント(ノートPC)の導入			
12	会社から、個人情報を含んだ印刷物の持ち込みを制限する			
13	印刷物へ強制的に印刷者の情報透かしを挿入			
14	IDSを設置しサーバ等に攻撃が行われていないか監視する			
15	会社に入るための入退出管理(カード式)システムを採用する			○

Fig. 2: The display of the optimized solution with MRC-Lite

Table 2: Index of the degree of burden on convenience and privacy

Degree of burden on convenience (0-9) Degree of burden on privacy (0-9)	How does the participant feel?
0-3	Hardly unpleasant
4-6	Slightly unpleasant
7-9	Unpleasantness

4. Application of MRC-Lite for the Personal Information Leakage Problem

4.1. Risk Communication Experiment of MRC-Lite

As an experiment of possible risk communications to compare MRC-Lite with MRC, risk communications were held with a model called "the personal information leakage problem in the company." Taniyama et al. [6] conducted a similar experiment with the MRC, and the result is used here for the comparison. However, this time, we also had risk communications by two groups of three students of Tokyo Denki University using MRC-Lite, not the MRC. All of them had knowledge of the MRC. In the trial application, the risk communications were started with determination of the proposed countermeasures, as presented in Section 3.2. The role players and the countermeasures are listed in Tables 3 and 4, respectively.

Table 3: Role players

1.	Employee
2.	Customer
3.	Manager

Table 4: Countermeasures

1.	Configure the system to change their password mandatorily four times a year.
2.	Install management software indicated by the manager to prohibit running unauthorized software that

	the manager does not allow.
3.	Install management software to prohibit using portable devices for the server.
4.	Install a surveillance camera in the office to observe suspicious behaviors.
5.	Install a URL filtering tool to prevent the use of web-based email and postings for the message board.
6.	Install a mail filtering tool to restrict sending and receiving email. (Employees cannot send email out of the company without sending copies of the mail to their manager.)
7.	Install a mail filtering tool to restrict sending and receiving email. (Employees cannot send email containing an attached file out of the company without sending copies of the mail to their manager.)
8.	Install management software to encrypt the data automatically when employees try to copy the data from their desktops or laptop computers to portable devices. (They cannot decode the data without a computer in the company.)
9.	Distribute USB memory devices which encrypt the data automatically to all of the employees.
10.	Encrypt the data in the HDD of the laptop computers.
11.	Distribute thin clients to employees.
12.	Restrict taking printed personal information out of the company.
13.	Install a system which mandatorily puts watermarks on the printed information.
14.	Install an intrusion detection system.
15.	Install a security scanning system at all of the entering and leaving entrances for the company.

The results of the non-adopted proposed countermeasures were as follows.

4.1.1 Non-adopted proposed countermeasures

- Cost of countermeasures: 0 yen
- Burden on employee's convenience: 0
- Burden on employee's privacy: 0
- Countermeasures: none
- Qualitative leak risk: 18

The manager insisted on the adoption of proposed countermeasures 4, 7, 10 as countermeasures to the personal information leakage problem. In addition, he mentioned that he did not want to adopt proposed countermeasure 11 due to its high cost. The employee decided not to adopt the proposed countermeasure 11 in accordance with the manager’s opinion.

From the view of the burden on convenience and privacy, the employee insisted that he did not want to adopt proposed countermeasure 6. Consequently, the customer and the manager did not accept the adoption of proposed countermeasure 6.

The customer mentioned that he did not clearly know the value of the qualitative leak risk he set, so the value was not a constraint. The result is optimized solution A.

4.1.2 The constraint functions

- Countermeasures to adopt: 4, 7, 10
- Countermeasures not to adopt: 6, 11

4.1.3 Optimized solution A

- Cost of countermeasures: 152,564,750 yen
- Burden on employee's convenience: 24
- Burden on employee's privacy: 8
- Countermeasures: 4, 5, 7, 8, 10, 12, 13, 14, 15
- Qualitative leak risk: 0.10342

The customer found the result of the qualitative leak risk to be sufficiently low, and therefore the customer was satisfied with the result. However, the constraints of the cost were set as follows, because the manager insisted that the cost was too high. The result under these constraints is optimized solution B.

4.1.4 The constraint functions

- Countermeasures to adopt: 4, 7, 10
- Countermeasures not to adopt: 6, 11
- Cost of countermeasures: 120,000,000 yen

4.1.5 Optimized solution B

- Cost of countermeasures: 109,236,500 yen
- Burden on employee's convenience: 23

- Burden on employee's privacy: 7
- Proposed countermeasures: 4, 5, 7, 8, 10, 12, 14, 15
- Qualitative leak risk: 0.17062

The result of optimized solution B made the qualitative leak risk higher. However, the customer was satisfied with optimized solution B because the qualitative leak risk was within the tolerance level. As the constraint functions remained within the predictable, the manager was satisfied with the result. The employee thought that burden on the employee's convenience and privacy was a little high. However, the employee agreed with optimized solution B because the constraint functions that he did not want to accept were not adopted and optimized solution B was a lower burden on the employee's convenience and privacy than optimized solution A was. Therefore, optimized solution B was adopted and succeeded in consensus formation among the participants.

4.2. Evaluation of MRC-Lite

Using MRC-Lite for the risk communications was faster than using the MRC to obtain the optimized solution. Also, it was possible to compare the optimized solutions, so that we were able to conduct smooth risk communications. MRC-Lite was able to form a consensus in approximately 40 minutes, whereas MRC took an average of 90 minutes. The results of a questionnaire given to the participants after the experiment are shown in Table 5. Because a consensus was formed finally, evaluations of the usefulness and the satisfaction of the optimized solution received a high score. However, evaluations of the easiness to see the layout and the convenience received a low score. Therefore, we found that it is necessary to improve the display interface in the future. In addition, the following questions for MRC-Lite were written in the free description field.

- We do not know how to run a risk analysis and to set the parameters when a problem is analyzed from scratch.
- We do not know the effectiveness of the value of the qualitative leak risk.

It is thought that a user manual is necessary to solve problem (1). Problem (2) is settled by determining an index of the value of the qualitative leak risk.

Table 5: Questionnaire result (evaluation: 1-5)

Details	Evaluation (n=6)
An evaluation of the usefulness of MRC-Lite	4.0
An evaluation of the satisfaction of the optimized solution	4.2
An evaluation of the easiness to see the layout	3.6
An evaluation of the convenience of MRC-Lite	3.6

5. Conclusion

In this paper, the status of development of MRC-Lite, which is a simplified version of the MRC, and the result of a trial application of MRC-Lite were reported. We found that smooth risk communications are possible by using MRC-Lite. However, the qualitatively valued derivative risk was not easy to understand as the constraint function. Therefore, it is necessary to make an index of the value. In addition, improvement of the layout is necessary.

In future work, we will improve the layout and apply MRC-Lite to other problems in addition to the information leakage problem.

6. 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 Communicator”, Risk Analysis 2008.

[3] Tabuchi Haruki ” Security technique of the information security by the international standard”

[4] Method of the risk estimate (example of the matrix method)

www.mhlw.go.jp/bunya/roudoukijun/anzeneisei14/dl/080301b_0010.pdf

[5] IT information management FTA(fault tree analysis)
http://www.atmarkit.co.jp/aig/04biz/fta.html

[6] Takashi Moriya, Yuu Hidaka, Masato Arai, Satoshi Kai, Hiromi Igawa, Hiroshi Yoshiura, Ryoichi Sasaki "Application of "Multiple Risk Communicator" to the Personal Information Leakage Problem in the enterprise "CSS2008, (2008)