Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking

Kiyoshi Nagata
and
Michio Amagasa

Faculty of Business Administration
Daito Bunka University
1-9-1 Takashimadaira
Itabashi-ku, Tokyo
175-8571, Japan
e-mail: nagata@ic.daito.ac.jp

Yutaka Kigawa

Faculty of International Communication
Musashino Gakuin University
860 Kamihirose
Sayama-city, Saitama,
350-1321, Japan

Dongmei Cui

Faculty of Business Administration and Information
Tokyo University of Science, Suwa
5000-1, Toyohira
Chino-city, Nagano
391-0292, Japan

Abstract

In an information-oriented society, the security of information related assets in organizations is one of chief concerns and the importance of security evaluation system to grasp their security level is increasing. We also consider that the magnitude of risk to information assets is highly dependent on the scales, forms, treat etc. of the organization, and should be evaluated by reflecting these characteristics. Standing on this concept, we adopted OCTAVE[SM] as the basic information system and already proposed two fuzzy-based methods integrated in it. One is to determine the set of critical assets using fuzzy decision making methodology by multi-participants. The other is to calculate the degree of risks along with the given threat path as a crisp value using fuzzy inference mechanism and so on. In this paper, we propose a system for selecting some mitigation controls considered to be more effective than others as an application of fuzzy outranking.

1. Introduction

In any kind of organization or company, the information system became one of most important systems to manage their business or non-business activities. On the other side, the information security concerned problems increased consequent on the spread of internet protocol based technologies and the rapid paradigm shift from closed information systems to open ones. In order to reduce the magnitude of information related risk, there are some types of information security evaluation and management systems. We studied several existing systems and concluded to adopt OCTAVE[SM] as our base system some part of which fuzzy-based methods are integrated.

We proposed a method to select the set of critical assets in the first phase of OCTAVE[SM] using Modified Structural Modeling Method, MSMM [6], and we also proposed an integrated system to evaluate the risk degree of given threat path from a critical asset as the starting point using fuzzy inference mechanism and so on.

The rest of this paper is organized as follows: in the next section we survey some information security evaluation and management systems. A brief instruction for OCTAVE[SM] and its basic risk profile for establishing the threats' identification are given in the following section. In the section 4, our method, already proposed in [8], to have integrated value of risk from impact values and probability with confidence level is briefly explained. Then we propose new method for selecting a set of effective mitigation controls for each of possible threat path in the following section.

2. General view of information security evaluation and management systems

The British Standards Institute (BSI) originally issued BS7799 in 1993 as a standard for information security management under the title of "Code of Best Practice, Information Security Management" and published in 1995, then also published as the replaced version in 1999. This standard had two parts. The part 1 is on the information technology, Code of practice for information security management. The part2 is on the Information Security Management Systems(ISMS). In 2005, the part3 was published covering risk analysis and management. ISO/IEC 17799 is established in 2000 as a guideline for information security management practice complying with the part1 of BS7799 having the 12 sections as follows: Scope, Terms and Definitions, Security Policy, Security Organization, Asset Classification and Control,

978-0-7695-3872-3/09 $26.00 © 2009 IEEE
DOI 10.1109/ISDA.2009.186

Personal Security, Physical and Environmental Security, Communications and Operations Management, Access Control, System Development and Maintenance, Business Continuity Management, and Compliance. In Japan, we have a standard JIS X 5080 defined by Japanese Industrial Standard Committee (JISC) related to ISO/IEC 17799. In 2005, ISO replaced it by ISO/IEC 27002 and JIS X 5080 was also replaced by JIS Q 27002.

ISO established ISO27001 complying with the part2 of BS7799, which essentially explains how to apply ISO 17799. The part 2 defines a six part of process: Define a security policy, Define the scope of the ISMS, Undertake a risk assessment, Manage the risk, Select control objectives and controls to be implemented, Prepare a statement of applicability.

In Japan we have an ISMS Certification Criteria also based on the part2 of BS7799. According to Japan Information Processing Development Corporation (JIPDEC), the certificate body for the ISMS, there are 9 steps for establishing ISMS as follows; (1) Define the range to which the ISMS applies: In terms of the characteristic, organization, location, assets, and technology of the business operation, (2) Planning ISMS policies: In terms of the characteristics, organization, location, assets, and technology of the business operation, (3) Planning a systematic approach to risk assessment, (4) Identifying risks (5) Performing risk assessment, (6) Performing risk treatment, (7) Selecting management goals and controls, (8) Preparing a statement of applicability, (9) Approving residual risks and following ISMS to be carried out. The number of organizations obtained the ISMS certification in Japan steadily increased from 420 in 2004 to 3149 in 2009.

We have another Risk Management System, called JRMS(JIPDEC Risk Management System) developed by JIPDEC, aiming to analyze the risk management system of an organization and to clear up their information security related matters. The main measure of JRMS is the vulnerability analysis based on a maturity model. Obtained information by means of a questionnaire consists of more than 1000 items are classified into 4 or 5 layers from various levels of position, then the items are summarized according to the top level ones. The output is a set of radar charts which might describe the gaps between the present state of the organization's information security related management systems and their ideal matured models.

JRMS is a risk analysis and management system focused on the management of organization or company. ISO/IEC 27002, JIS Q 27002, and other BS7799 part1 originated systems are standard for the management of information security which gives us a guideline for managing the information system in the perspective of securities. BS7799 part2 originated ISO27001 and ISMS are the certification systems which might give organizations the public reliability on managing the information assets. Another merit of obtaining these certifications is to encourage the awareness of personnel on the information security and to understand the system to manage their information assets through the process of preparing for the certification.

We briefly refer to MEHARI, MAGERI, and NIST800-30 as important methodologies in our concerned area. MEHARI is one of important contributions of CLUSIF(Club de la Sérurité de L'information Français, France) to the management of Information related risks, whose English translation is "Harmonized Risk Analysis Method". MEHARI provides a consistent set of tools and methods with appropriate knowledge databases for security management required by some of standards such as ISO13335, ISO/IEC 27002. Chief information security officers, general managers, and security managers or other information related risk concerned people are assumed users. Its document is available in http://www.clusif.asso.fr/en/clusif/present/.

MAGERIT is promoted by CSAE(Consejo Superior de Administración Electrónica, Spain) as a information security management system directly related to the generalized use of electronic, computerized and telecommunication media which are subject to be endangered by risks. The English translation of MAGERIT is "Methodology for Information Systems Risk Analysis and Management". They state that MAGERIT seeks to achieve (1) To make those responsible for information systems aware of the existence of risks and of the need to treat them in time, (2) To offer a systematic method for analyzing these risks, (3) To help in describing and planning the appropriate measures for keeping the risks under control, (4) To prepare the organization for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case. Its document is available in http://www.csi.map.es/csi/pg5m20.htm. NIST 800-30 is published by NIST(National Institute of Standards and Technology, US) as "Risk Management Guide for Information Technology Systems", which aims to provide a foundation for the development of an effective risk management program. In the program, both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems are contained. We can get the guide from http://csrc.nist.gov/.

We ultimately aim to integrate some methods for decision making, problem solving etc. into a good information security evaluation system. For this purpose, we consider the system should be able to

manage the human's ambiguity, on the other side it should systematically complete. Eventually, we adopt OCTAVE[SM] which will be explained in the following section as the base system, and introduce fuzzy concept. Since OCTAVE[SM] bases on the organizational assets, and the critical assets are one of very important components to evaluate their information system, we proposed a method to extract them using our MSMM [6][7]. We also proposed a method to evaluate risks along with a threat path in the work sheet of OCTAVE[SM] with fuzzy inference mechanism [8].

3. OCTAVE[SM]

OCTAVE[SM] (Operationally Critical Threat, Asset, and Vulnerability Evaluation System) was developed by SEI (Software Engineering Institute) of Carnegie Melon University as a security evaluation system based on organizational assets [1]. OCTAVE-S is a variation of the approach tailored to relatively small organizations(less than 100 people) which have the limited means and unique constraints.

In the implementation guide [2], four key features such as Organization evaluation, Focus on security practices, Strategic issues, Self direction are mentioned. They pointed out that some other evaluation systems are tend to evaluate the organizational systems and to focus on the technology. Though the technology is one of three important key aspects for risk assessment, other two aspects (operational risk and security practice) mainly drive OCTAVE approach and the technology is examined as the part of security practice. OCTAVE aims to evaluate the organization itself in aspect of information assets, threats, and vulnerabilities and focus on their practices to obtain the information security, which eventually lead the organization to strategic protection issues rather than tactical ones. The expert led system is managed by a team of experts in risk analysis, information technologies outside or inside. OCTAVE is self-directed system lead by a small interdisciplinary team, called an "analysis team", consistent of members in the organization.

OCTAVE(-S) has three phases in each of which the corresponding outputs as follows are expected.

Phase1. Build Asset-Based Threat Profiles
Outputs: Critical assets, Security requirements for critical assets, Threats to critical assets, and Current security practices

Phase2. Identify Infrastructure Vulnerabilities
Outputs: Key components and Current technology vulnerabilities

Phase3. Develop Security Strategy and Plans
Outputs: Risks to critical asset, Risk measures, Protection Strategy, and Risk mitigation plans

Each phase has some process consist of several steps, which we show in the table1 from the guide.

Table 1. Phase, Process, and Group of Steps in OCTAVE-S

Phase	Process	Group of Steps
Phase1	S1:Identify Organizational Information	S1.1:Establish impact evaluation criteria S1.2:Identify organizational assets S1.3:Evaluate organizational security practices
	S2:Create Threat Profiles	S2.1:Select Critical Assets S2.2:Identify security requirements for critical assets S2.3:Identify threats to critical assets
Phase2	S3:Examine the Computing infrastructure in Relation to Critical Assets	S3.1:Examine access path S3.2:Analyze technology-related process
Phase3	S4:Identify and Analyze Risks	S4.1:Evaluate impact of threats S4.2:Establish probability evaluation criteria S4.3:Evaluate probabilities of threats
	S5:Develop Protection Strategy and Mitigation Plans	S5.1:Describe current protection strategy S5.2:Select mitigation approaches S5.3:Develop risk mitigation plans S5.4:Identify changes to protection strategy S5.5:Identify next steps

We adopt the Basic Risk Profile of OCTAVE(-S) to identify the threats corresponding to S2.3, S.4.1, and S4.3 in the table 1. Threats are classified into three types such as "Human actors", "System problems", and "Other problems" in the first place. For the "Human actors" causing threats, the "Access path" (network or physical), "Actors" (inside or outside), "Motive" (accidental or deliberate), and "Outcome" (disclosure or modification or loss and destruction or interruption) are examined in this order. For the "System problems" causing threats, "Actors" (software defects or system crashes or hardware defects or malicious code), and "Outcome" are examined. For the "Other problems", various "Actors" (e.g. problems related to power supply, telecommunication, third-party, natural disasters, physical configuration etc.) are

examined.

Figure 1 is an example of the work sheet of type of "Human actors". Each impact area of "Reputation", "Financial", "Productivity", "Fines/legal penalties", "Safety" and "Other(facilities)" are considered for the non-negligible threats as the result of examination. According to the volume 3 of the OCTAVE-S Implementation Guide, the three impact measures (High, Medium, or Low) are adopted, and probability values are also measured as one of them(H, M, or L) by considering a frequencies such as "daily", "weekly", "monthly", "4 times per year", "2 times per year", "once per year", "once very 2 years", and so on. Figure 1 is an example of the thread profile worksheet for the "Human Actors Using Network Access".

4. Risk evaluation method along with definite threat path

We have proposed a method to evaluate the risk along with the OCTAVE's threat path [8]. In figure 1, once an asset was set in the left-side box, all the possible paths are investigated in the first place, then the impact values and the probability with its confidence level are written in. We assume that those values are numerically given by some kind of criteria instead of linguistic values. Our method consists of two aggregation techniques, one is for the impact values and the other is for the probability, in each of which the organization's characteristic and the asset's properties are considered respectively before they are integrated. For the integration of impact values, we adapted the MSMM to have the consented structure of impacts and the weight vector. For the integration of probability and its confidence level, we adapted the fuzzy inference mechanism to obtain the probability value with confidence degree.

5. Method to select effective risk mitigation controls

In our previous work, we already proposed a method to calculate numerical evaluation values along with each threat path from a given asset. These values are helpful for giving priorities of each threat path to be managed by some mitigation controls.

Now we propose a method to select a set of efficient mitigation controls using the fuzzy outranking method under the assumption that we have an external data base of mitigation controls with some kind of mitigation value.

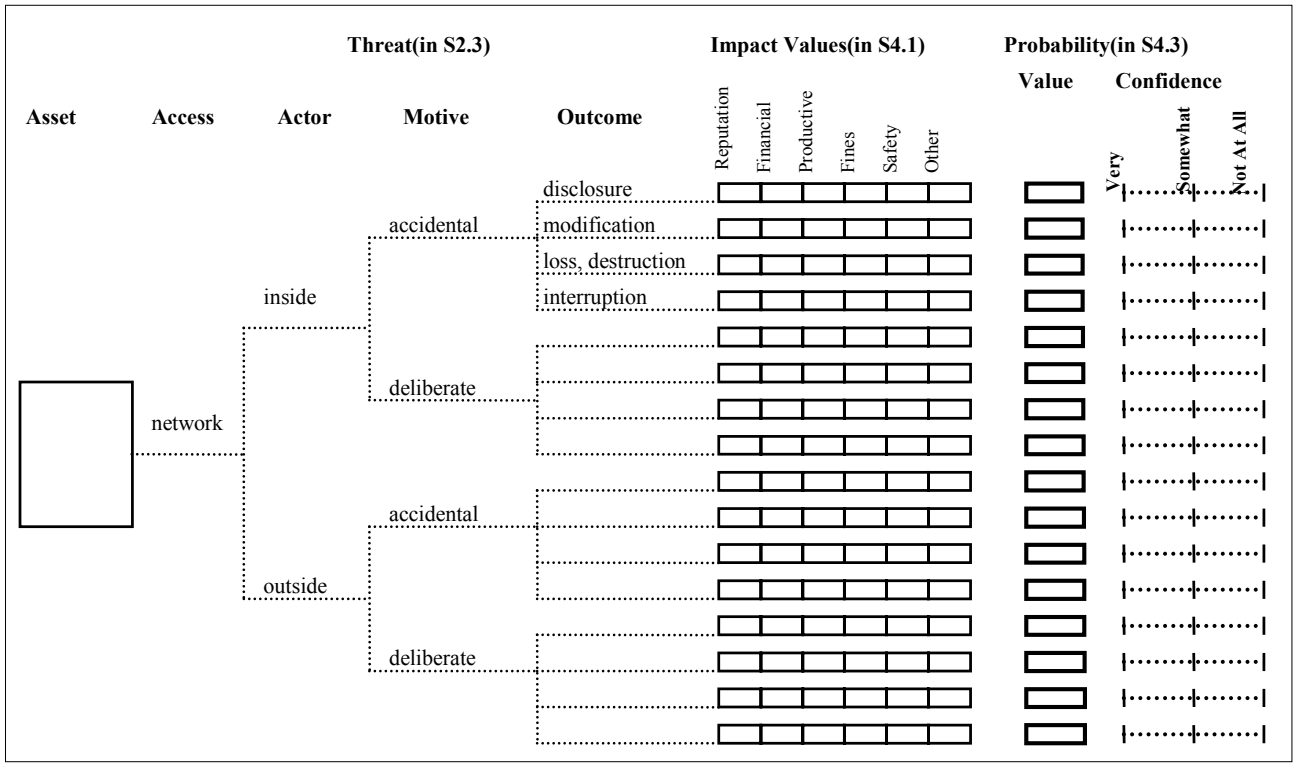

Figure 1. Risk Profile work sheet (source: the Vol. 5 of OCTAVE-S Implementation Guide)

5.1. Fuzzy outranking method

The method to roughly compare two alternatives a and a' through the adoption of loose relation is called outranking. When a is judged not to be inferior to a' at least, it is said that a outranks a'. When a' is more preferable than a or they are incomparable to each other, it is said that a doesn't outrank a'. While these relations are valued as 0 or 1 in the conventional

outranking method, such as $\mu(a,a')=1$ if a outranks a' and $\mu(a,a')=0$ if a does not outranks a', the fuzzy outranking method access the outranking degree as a value between 0 and 1. More precisely, that degree is determined using a fuzzy membership function with lower threshold value q_i and upper one p_i, where "i" represents one of view points for evaluating these alternatives. Thus the corresponding value is denoted by $c_i(a,a')$ ($i=1,\ldots,n$), and they are aggregated by taking the weighted average $\omega_1 c_1(a, a')+\cdots+\omega_n c_n(a, a')$ with a set of certain weight $\{\omega_1,\ldots, \omega_n\}$. This index is called the "concordance index" denoted by $C(a,a')$. Another index is "discordance index" denoted by $d_j(a,a')$, which is also calculated using a fuzzy set with lower threshold value p_j and upper one v_j. This index represents the degree of objection against the preferability to choose a then a'. Thus $d_j(a,a')=1$ implies that the condition "a outranks a'" is exclusively vetoed from the number j point of view.

If there are discordant points of view $j_1,\ldots, j_k$, whose index are greater than $C(a,a')$, then the total outranking index $\mu(a,a')$ is calculated by the following formula,

$$\mu(a,a')=C(a,a')\times\frac{1-d_{j_1}(a,a')}{1-C(a,a')}\times\cdots\times\frac{1-d_{j_k}(a,a')}{1-C(a,a')}.$$

5.2. Our proposal method

Now we propose our method for selecting set of mitigation controls from a database of controls. As a prerequisite, we assume the existence of an external database, D, of mitigation controls with mitigation degree, $\delta_m(T)\in[0,1]$ and $m\in D$, evaluated depending only on the type of threat path T. This mitigation degree should signify that adopting the control roughly mitigate the risk level from 1 to that degree.

As we explained in the section 4, we suppose that we have determined the set of critical assets and all the possible threat path were distinguished with the risk value calculated from $(v_R,v_F,v_P,v_{Fi},v_S,v_O,p)$, the vector of impacts and probability. This is the preliminary stage of our method.

Then the process is performed according to the following steps.

Step 1. Determine a threat path T.

Step 2. Select several controls as members of the candidate set, $M\subset D$, by evaluating their initial mitigation degree dependent on T. One simple way to determine M is setting $M=\{m\in D: \delta_m(T)<\delta\}$ for a definite value δ.

Step 3. Define the desirable, but dummy, mitigation control, a_0, as an acceptable impacts and probability vector $(v_R^0,v_F^0,v_P^0,v_{Fi}^0,v_S^0,v_O^0,p^0)$.

Step 4. For each element $m_j\in M$, figure out its mitigation degree $d_*{}^j$ with respect to each of impacts and probability. For instance, $d_R{}^j$ represents the reduction degree with respect to the impact of reputation when m_j is performed. These degrees are calculated by considering the type of assets, threat path, and impact or probability in some criteria.

Step 5. Calculate $a_j=(v_R{}^j,v_F{}^j,v_P{}^j,v_{Fi}{}^j,v_S{}^j,v_O{}^j,p^j)$ as the alternative vectors corresponds to m_j by $d_*{}^j\times v_*$.

Step 6. Apply the fuzzy outranking method with certain threshold values of concordance and discordance indices to each of (a^j,a^0) for $j=1,\ldots n$, where n is the cardinality of M.

Step 7. Determine the set of effective mitigation controls E_T by referring the values $\mu_i=\mu(a^j,a^0)$. We have two versions for this. One is to determine $E_T=\{m_j;\ \mu(a^j,a^0)>\alpha\}$ as the optimal set with fixed lower boundary value α. The other is to choose the definite number of m_is' from the permutated mitigation controls in descending order.

6. Illustrative Example

We set one of critical assets in figure 1 and consider a threat path T="network-inside-accidental-disclosure" from the asset. Suppose that the candidate set M is already selected by means of $\delta(T)$.

Table 2 illustrates the corresponding values. In the second row, evaluated weight using MSMM are written in. The current threat levels are given as a number between 0 and 10. The optimal levels are in a_0-row, and mitigation degrees of certain control are in a_1-row. Then the outranking values corresponding to each impact, $\mu_i(a^j,a^0)$ (i=R,F,…,O), are calculated with a pair of lower and upper threshold values q_i, p_i. Here we set $(q,p)=(0.5,2)$, and outranking method are performed to see each of mitigated values outranks corresponding optimal ones. The values in the right column are weighted averages, and resulted outranking value in the lower right is 0.614.

Although the table 2 is just for impact, we calculated the outranking value for the probability, setting 0.35 as the current value, which is resulted by fuzzy inference mechanism from the probability 0.1 and the confidence level 0.5 [8]. Supposing that the control's mitigation degree is 0.63, we use this value for the probability mitigation degree. When the optimal value is 0.2, and $(q,p)=(0.01,0.06)$, the resulted value is 0.79. We configured the probability as the discordant index, but that does not affected in this case.

Thus the integrated value, the average of 0.614 and 0.79, is 0.683.

Table 2. Outranking for Impact values

	v_R	v_F	v_P	v_{Fi}	v_S	v_O	VI
weight	0.35	0.25	0.05	0.1	0.2	0.05	1
current threat level	8	8	3	5	3	2	6.15
a_0	5	5.2	6	3	2.5	6	4.45
a_1	0.8	0.75	0.8	0.75	0.85	0.2	
mitigated value	6.4	6	2.4	3.75	2.55	0.4	4.77
$c_i(a_1,a_0)$	0.6	0.2	1.0	0.167	1.0	1.0	0.614

7. Conclusion

In this paper, we proposed a new method to select effective mitigation controls against information security risk from a large database. Although the method was discussed in the series of works based on OCTAVE[SM], our method can be applied in many kinds of information security related evaluation and mitigation methodologies.

In order to complete our system, we should point out that the following two defects are to be settled.

(1) Make a large database of the potential mitigation controls with the mitigation degree depending on each threat path, or develop a method for calculating the degree as a function from the database into the interval [0,1].

(2) Design or construct a system for evaluating the mitigation degree of each impact and probability for a selected mitigation control and fixed threat path from a given asset.

Making the database is a big project which requires long time and a plenty of workload. It might be an endless work since new mitigation controls are to be contrived with time.

As the implementation of OCTAVE[SM] is led by an analysis team whose members are from several department of the organization, the evaluation of mitigation controls can be performed by them using some of ordinary method. We intend to propose a systematic scheme for the evaluation as our future work.

8. References

[1] Alberts, C. and Dorofee, A., *Management Information Security Risks*, Addison-Wesley (2003)

[2] Alberts, C., Dorofee, A., Stevens, J., and Woody, C., *OCTAVE-S Implementation Guide*, Version 1.0, CMU/SEI-2003-HB-003(2005)

[3] Gabus, A. and Fontela, E., *DEMATEL Reports*, Battelle Geneva Research Centre(1975)

[4] Kaufman, A. et al., *Introduction to the Theory of Fuzzy Subsets*, NewYork: Academic Press(1975)

[5] Klir J. George and Yuan Bo, *Fuzzy Sets and Fuzzy Logic-Theory and Application*, Prentice Hall InternationalInc. pp124-132(1995)

[6] Nagata, K., Umezawa, M., Cui, D., and Amagasa, M., "Modified Structural Modeling Method and Its Application - Behavior Analysis of Passengers for East Japan Railway Company-", *Journal of Industrial Engineering & Management Systems*, Vol. 7, NO. 3, pp.245-256(2008)

[7] Nagata, K., Kigawa, Y., Cui, D., and Amagasa, M., "Integrating Modified Structural Modeling Method with an Information Security Evaluation System", *Proceedings of the 8th Asia Pacific Industrial Engineering and Management Systems Conference 2007*, T1-R02, ID68(2007)

[8] Nagata, K., Kigawa, Y., Cui, D., and Amagasa, M., "Risk Evaluation for Critical Assets with Fuzzy Inference Mechanism in an Information Security Evaluation System", *Proceedings of the 9th Asia Pacific Industrial Engineering and Management Systems Conference 2008*, pp.2630-2640(2007)

[9] Tazaki, E. and Amagasa, M., "Structural Modeling in a Class of Systems Using Fuzzy Sets Theory", *International Journal of Fuzzy Sets and Systems*, Vol.2, No.1, pp.87-103(1979)

[10] Vlacic, L., Amagasa, M., Ishikawa, A., Williams, T. J., and Tomizawa, G, "Applying Multiattribute-Based Group Decision Making Techniques in Complex Equipment Selection Tasks", *Group Decision and Negotiation*, 6, pp. 529-556(1997)

[11] Zadeh, L.A., "Fuzzy Set", In *Information and Control*, Vol.8, pp.338/353(1965)