Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 14 (16): 1865-1870, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1865.1870

On Multi Attribute Decision Making Methods: Prioritizing Information Security Controls

Nedher AL-Safwani, Suhaidi Hassan and Norliza Katuk
Inter Networks Research Laboratory, Universiti Utara Malaysia, Malaysia

Abstract: This study deals with the problem of prioritization of Information Security Controls where most organizations aim to address and manage them effectively. Current information security analysis methods lack a quantitative approach and mostly depend on subjective judgments of information security experts. Although, expert opinions assist organizations in measuring the effectiveness of security controls, the subjective judgments may yield different results. Hence, a more objective approach that can be quantified is an alternative. This study implements multiple attribute decision-making concepts for prioritizing and selecting security controls using Hierarchical Adaptive Weighting (HAW) and Simple Adaptive Weighting (SAW). The results of these analysis methods are reported and compared.

Key words: Information security controls assessment, information security controls, multiple attribute decision making, security controls analysis

INTRODUCTION

The focus of information security is to protect organizations from attacks and to provide confidentiality, integrity, availability, authenticity and non-repudiation (CIAA) of their information assets (Wheeler, 2011). A continued defense technique against threats on these assets can be achieved through control assessment and analysis methods. Many organizations have seen these as a priority and they have becoming increasingly important to minimize the potential risks (Feng and Li, 2011; Lv *et al*., 2011).

Information security experts urge organizations to conduct information security risk assessment to preserve the CIAA of the assets and to help them meet business objectives (Gordon and Loeb, 2006). Several approaches are available on the process aspects of risk management covering from standards organizations, academic groups, to industry bodies. These approaches include ISO27005 (ISO/IEC, 2008), NIST SP 800-30 (Stoneburner *et al*., 2002), OCTAVE (Alberts *et al*., 2003), Information Risk Analysis Methodology (IRAM) (IRAM, 2010; IRAM, 2011), CRAMM (Veiga and Eloff, 2007) and expression of needs and identification of security objectives (EBIOS) (EBIOS, 2010). These approaches provide a process framework and allow organizations to define their analysis process in selecting and prioritizing security controls (Singh, 2009). Most of these frameworks are also based on qualitative analysis and require real experts to follow the complicated steps for selecting the best and critical controls (Andersen, 2009; Hubbard, 2009). This situation has encouraged researchers to improve security decisions of the framework by applying quantitative or qualitative modeling techniques (Lauesen and Younessi, 1998).

Risk assessment research was expanded in the last few years, both in the academic and commercial sectors but the key area of IT risk assessment is yet to receive enough attention (Breier and Hudec, 2011). Several risk analysis methodologies and models were developed to solve the issues and challenges of these methods (Kiesling *et al*., 2012). However, quantitative techniques and methods that consider decision-making criteria and cost effective analysis are still lacking.

Early work in this area was proposed by (Singh and Lilja, 2009), where by a statistical design of experiments based on security architecture was presented. The authors generated the security control configuration change recommendations based on the cost criteria that are important to the enterprise and the changing nature of threats. A statistical model scored the critical controls based on the simple sum of ranks of the cost criteria, wherein an inaccurate evaluation can be created.

The major contribution of (Lv *et al*., 2011) is a control-ranking model that considers multiple criteria analysis and the interests of different decision makers in implementing a security control plan. However, the authors ignored the feature of the control ranking problem as a group decision problem where subjective and objective judgment must be available to provide better ranking to controls. The Cyber Investment Analysis Method was proposed by Llanso (2012). A data-driven approach for selecting and prioritizing security controls provides a frame work to rank the security controls. The framework ranks the security controls based on the data

Corresponding Author: Nedher AL-Safwani, Inter Networks Research Laboratory, Universiti Utara Malaysia, Malaysia

set extracted from previous experiments and control effectiveness scoring. The methodology mainly focuses on prioritizing the controls based on the control effectiveness score. In setting the security controls, however, weighting is computed based on subject matter experts who used their knowledge of security control capabilities. These weights are based on expert observations about the effectiveness of controls. Clear classification of the data set and the analysis and estimation is not available.

MULTI ATTRIBUTE DECISION MAKING

Multiple criteria decision making (MADM) refers to decision-making in the presence of multiple, confusing or conflicting criteria. Multiple criteria decision problems are common (Hwang and Yoon, 1981; Zavadskas *et al*., 2009). MADM methods are classified into three 2 types based on the type of information that the decision maker provides: no information, information on attributes and information on alternatives (Hwang and Yoon, 1981; Yoon and Hwang, 1995; Kahraman and Ceb, 2009). This study ocuses on the type of information where the decision maker provides information on the attribute. Hierarchical Adaptive Weighting (HAW) and Simple Adaptive Weighting (SAW) are some of the major classes of the information on attributes methods of MADM. Therefore HAW and SAW are selected and applied in this study. Multiple attribute decision-making ranking defines fundamental terms such as decision matrix, the Evaluation Matrix (EM), the alternatives and the criteria.

The evaluation matrix consisting of alternatives m and n criteria need to be created, with the intersection of each alternative and criteria given as x_{ij} we therefore have a $(x_{ij})m.n$:

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \end{array}$$

where $A_1, A_2,..., A_m$ are possible alternatives among which decision makers have to choose (i.e., technical security controls), $C_1, C_2,..., C_n$ are criteria with which alternative performance are measured (i.e., vulnerabilities, threats, valid vulnerabilities, severity, cost remediation effort) and finally, x_{ij} is the rating of alternative A_i with respect to criterion C_j and W_j is the weight of criterion C_j (i.e., threats weight, severity weight and cost remediation weight). A certain processes need to be done to rank the alternatives such as normalization, maximization indicator, adding the weights and other processes depend on the method.

Hierarchical adaptive weighting (HAW method)

Rescoring: In the hierarchical additive weighting method (HAW) each criterion value interprets x_{ij} the ratio of as the sub-score of the alternative ith with regards to the jth criterion, which is defined as:

$$k_j = x_{ij} / \sum_{i=1}^{4} x_{ij}, \quad j=1, 2,..., n \tag{1}$$

$$k_j = \frac{1}{x_{ij}} / \sum_{i=1}^{4} \frac{1}{x_{ij}}, \quad j=1, 2,..., n \tag{2}$$

Equation 1 is used when there is benefit criteria, while Eq. 2 used when there is cost criteria. This will result the new matrix K:

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{bmatrix}$$

Ranking the alternatives based on the mission effectiveness: Assume the set of weights A_i from the decision maker is accommodated, to compute the vector for the hierarchical mission effectiveness h is given by:

$$h = k^{*}w^{T} \tag{3}$$

where, (w^T) is the transpose of vector (w).

Ranking the alternative according to the descending value of the alternatives: The set of alternative A_i can now be ranked according to the descending order of the alternatives, where, the highest value the better performance.

Simple adaptive weighting (SAW method)

Linear scale transformation: In this process, the value of the criterion is divided by the maximum value of the criterion for all alternatives, therefore:

$$r_{ij} = x_{ij}/x_j^{*} \tag{4}$$

$$r_{ij} = \min x_{ij}/x_{ij} \tag{5}$$

Equation 4 is used when there is benefit criteria, while Eq. 5 used when there is cost criteria. This will result the new matrix R:

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{bmatrix}$$

Construct the weighted transformed decision matrix: In this process, a set of weights $w = w_1, w_2, w_3,..., w_j,..., w_n$, from the decision maker is accommodated to the transformed decision matrix; the resulted matrix can be calculated by multiplying each column from normalized decision matrix (R) with its associated weight w_j. As mentioned before the set of the weights is equal to 1, this process will result a new matrix V where, V is as shown below:

$$V = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1r_{11} & w_2r_{12} & \cdots & w_nr_{1n} \\ w_1r_{21} & w_2r_{22} & \cdots & w_nr_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{m1} & w_2r_{m2} & \cdots & w_nr_{mn} \end{bmatrix}$$

Construct the weighted average value for the alternatives: In this process, the summation of the new values that resulted from the previous step is calculated as:

$$A_i^* = \sum_{j=1}^{6} v_{ij},\ j = (1, 2, ..., n) \quad (6)$$

Ranking the alternative according to the descending value of the alternatives: The set of the alternative A_i can now be ranked according to the descending order of the alternatives, where, the highest value the better performance.

RESULTS

This section presents the results obtained from the prior experiments conducted in a small-medium enterprise, where indifferent technical security controls are implemented. A small and medium enterprise in Malaysia was selected. This enterprise was an internet security consulting company that had less than 250 employees. Technical controls are defined as the safeguards built into the hardware and the computer software such as firewalls, routers, databases and servers. More than 50 experiments were conducted in a real-time network. The vulnerabilities among these controls were first identified using different vulnerability assessment tools such as Nessus, Nmap, Dumpsec, Kismet and Acunetix. The analyzed data were obtained from the vulnerability assessment using different penetration testing tools such as Metasploit, AirSnort and Nstealth. The data were validated to obtain accurate result estimation prior to the data analysis. A group analysis panel was conducted with different experts to estimate the severity and cost of the remediation effort. Security controls were rated on a scale of 1 (critical risk) to 18 (low risk). Finally, the obtained results were analyzed using the HAW and SAW methods to prioritize the feedback and data of the experts as shown in Table 1 and 2. The controls for each criterion shown in Table 1 were ranked using the HAW and SAW methods based on the high risk of the control (1 being the most critical and 18 being the least critical). The ranks for each criterion were then determined again using the HAW method to determine an overall rank. The top eight critical risks of the information security controls to the organization were selected. A comparison of the results in Table 1 and 2 reflected in Table 3.

Table 1: Results ranking summary of HAW method

Technical security controls	Known vulnerabilities	Valid vulnerabilities	Attack class	Severity	Remediation effort level	Ranking
Router	3	2	2	2	2	2
Firewall	17	16	16	18	13	18
Web application	1	1	1	1	1	1
Web server	2	3	4	4	3	3
DHCP server	9	11	6	14	9	8
Active directory	11	9	7	13	12	10
CCTV server	7	6	9	9	6	6
File server	14	12	12	11	10	12
Antivirus server	10	8	13	12	15	11
Database	4	7	10	10	8	7
Active mail server	8	10	14	5	14	9
Windows update server	15	15	15	17	16	17
VMware ESX server	5	5	5	3	4	4
Passive mail server	6	4	3	8	5	5
Wireless AP	15	17	17	6	17	15
Email gateway	18	18	18	7	18	16
DNS	12	13	8	15	11	14
Development server	13	14	11	16	7	13

Table 2: Results ranking summary of SAW method

Technical security controls	Known vulnerabilities	Valid vulnerabilities	Attack class	Severity	Remediation effort level	Ranking
Router	3	2	2	2	3	2
Firewall	17	16	16	18	7	16
Web application	1	1	1	1	1	1
Web server	2	3	4	4	2	3
DHCP server	9	11	6	14	10	9
Active directory	11	9	7	13	9	8
CCTV server	7	6	5	9	6	6
File server	14	12	10	11	12	12
Antivirus server	10	8	12	12	16	11
Database	4	7	9	10	13	7
Active mail server	8	10	14	5	15	10
Windows update server	15	15	15	17	17	18
VMware ESX server	5	5	11	3	4	5
Passive mail server	6	4	3	8	5	4
Wireless AP	16	17	17	6	14	15
Email gateway	18	18	18	7	18	17
DNS	12	13	8	15	11	13
Development server	13	14	13	16	8	14

Table 3: Comparison of HAW and SAW results

Technical security controls (HAW)	Technical security controls (SAW)
Web application	Web application
Router	Router
Web server	Web server
VMware ESX server	VMware ESX server
Passive mail server	Passive mail server
CCTV server	CCTV server
Database	Database
DHCP server	DHCP server
Active mail server	Active mail server
Active directory	Active directory
Antivirus server	Antivirus server
File server	File server
Development server	DNS
DNS	Development server
Wireless AP	Wireless AP
Email gateway	Firewall
Windows update server	Email gateway
Firewall	Windows update server

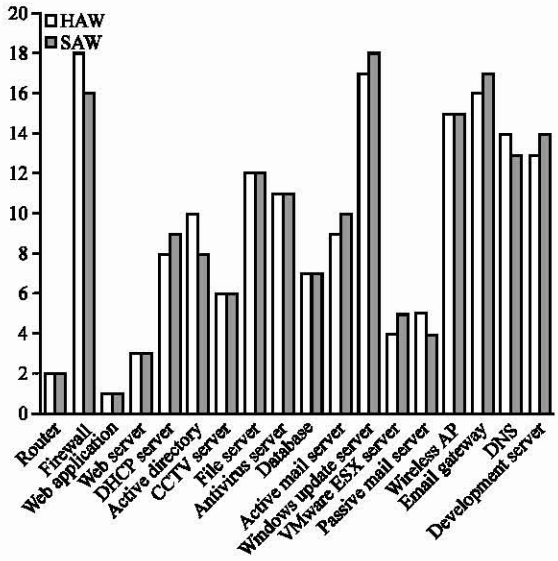

Fig. 1: Technical security controls ranking

DISCUSSION

Inaccurate selection and evaluation of information security controls can create an unclear view of organizational risk during the risk assessment exercise. The information security controls prioritization methods enable decision makers to formulate accurate decisions concerning the critical controls and threats that should be considered. The list of critical security controls in Table 1 shows that web application is the most important security control that should be addressed, followed by router, web server, VMware ESX server, passive mail server, CCTV server, database and DHCP server. These controls were evaluated based on the number of known vulnerabilities and based on different evaluation criteria, such as severity and cost remediation effort level. Critical controls were prioritized and selected using the SAW method as well, as shown in Table 2. The list of critical security controls in Table 2 shows that web application is the most vulnerable security control, followed by router, web server and VMware ESX server. A comparison of the results in Table 1 and 2 shows that the lists of these controls are slightly different, as reflected in Table 3. Table 3 shows that the two most significant controls of organization are the firewall and wireless AP for both methods. This result proves that the firewall, e-mail gateway server and Windows update server are the most effective controls in preventing attacks. Figure 1 shows the comparison ratio of HAW and SAW for technical security controls ranked from bottom to top.

CONCLUSION

Risk analysis is the fundamental basis of risk management and is the most important component in the

field of risk assessment. Information security experts in organizations conduct risk analysis through different phases to determine the levels of potential threats and the related risks to the assets of an organization. The current frameworks and methodologies are complex and full of uncertainty which can affect their effectiveness. The gap has encouraged many studies to improve the issues and challenges.

This study proposed MADM methods specifically HAW and SAW to enhance the information security control selection and prioritization. The solution proposed in this study improved the risk assessment process by providing a dynamic analysis method that will assist organizations to evaluate the ISC accurately while considering the weight of each attribute or evaluation criterion. It will also assist the organization covering and selecting the effectiveness performance of the security controls.

The data gathered in this study was obtained using different multi-decision attribute making methods. The results of this study and those of other methods should also be examined to determine the most effective method.

ACKNOWLEDGEMENT

Authors would like to thank the MPDSS community for theri valueable contribution to perform their result, Multi-purpose Decision Support System is a free simulation of individual and Group Multi Criteria Decision making techniques.

REFERENCES

Alberts, C., A. Dorofee, J. Stevens and C. Woody, 2003. Introduction to the octave approach. Technical Report 15213-3890, Carnegie Mellon University, Pittsburgh, USA.

Andersen, C., 2009. Successful security control selection using NIST SP 800-53. ISSA J., 1: 12-17.

Breier, J. and L. Hudec, 2011. Risk analysis supported by information security metrics. Proceedings of the12th International Conference on Computer Systems and Technologies, June 16-17, 2011, Vienna, Austria, pp: 393-398.

EBIOS, 2010. EBIOS 2010: Expression of needs and identification of security objectives. April 7, 2010. http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html

Feng, N. and M. Li, 2011. An information systems security risk assessment model under uncertain environment. Applied Soft Comput., 11: 4332-4340.

Gordon, L.A. and M.P. Loeb, 2006. Budgeting process for information security expenditures. Commun. ACM-Personal Inform. Manage., 49: 121-125.

Hubbard, D.W., 2009. The Failure of Risk Management: Why it is Brokenand How to Fix it. Willy, New Jersey, USA.

Hwang, C.L. and K. Yoon, 1981. Multiple Attribute Decision Making Methods and Applications. Springer-Verlag, Berlin, New York.

IRAM, 2010. Information risk analysis methodology risk assessment process. Internet, December 22, 2010.

IRAM, 2011. Information risk analysis methodology: Control selection. June 2011. https://www.securityforum.org/

ISO/IEC, 2008. ISO/IEC 27005:2008: Information technology. Security techniques. Information security risk management. http://shop.bsigroup.com/ProductDetail/?pid=000000000030117274

Kahraman, C. and S. Ceb, 2009. A new multi-attribute decision making method: Hierarchical fuzzy axiomatic design. Exp. Syst. Appl., 36: 4848-4861.

Kiesling, E., C. Strausss and C. Stummer, 2012. A multi-objective decision support framework for simulation-based security control selection. Proceedings of the 7th International Conference on Availability, Reliability and Security, August 20-24, 2012, Prague, pp: 454-462.

Lauesen, S. and H. Younessi, 1998. Six styles for usability requirements. Proceedings of the 4th International Workshop on Requirements

Engineering: Foundation for Software Quality, June 8-9, 1998, Pisa, Italy, pp: 155-166.

Llanso, T., 2012. CIAM: A data-driven approach for selecting and prioritizing security controls. Proceedings of the IEEE International Systems Conference, March 19-22, 2012, Vancouver, BC., pp: 1-8.

Lv, J.J., Y.S. Zhou and Y.Z. Wang, 2011. A multi-criteria evaluationmethod of information security controls. Proceedings of the 4th International Joint Conference on Computational Sciences and Optimization (CSO), April 15-19, 2011, Yunnan, pp: 190-194.

Singh, A. and D. Lilja, 2009. Improving risk assessment methodology: A statistical design of experiments approach. Proceedings of the 4th International Conference on Security of Information and Networks, October 2009, Sydney, Australia, pp: 21-29.

Singh, A., 2009. Improving information security risk management. Ph.D. Thesis, Minnesota University, Saint Paul, Minnesota.

Stoneburner, G., A.Y. Goguen and A. Feringa, 2002. Risk management guide for information technology systems. file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Downloads/NIST-800-30%252f800-66+Summary.pdf

Veiga, A.D. and J.H.P. Eloff, 2007. An information security governance framework. Inform. Syst. Manage., 24: 361-372.

Wheeler, E., 2011. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Elsevier, Waltham, ISBN: 9781597496162, Pages: 360.

Yoon, K.P. and C. Hwang, 1995. Multiple Attribute Decision Making. 1st Edn., Sage Publication, USA., pp: 83.

Zavadskas, E.K., A. Kaklauskas, Z. Turskis and J.E. Tamosaitien, 2009. Multi-attribute decision-making model by applying grey numbers. Informatica, 20: 305-320.