The Use of AHP in Security Policy Decision Making: An Open Office Calc Application

Irfan Syamsuddin [1*]
Department of Computer and Networking Engineering
State Polytechnic of Ujung Pandang,
Makassar, Republic of Indonesia
Email: irfans@poliupg.ac.id

Junseok Hwang
[1] International IT Policy Program (ITPP),
Technology Management, Economics and Policy Program (TEMEP),
Seoul National University,
Seoul, Republic of Korea
Email: junhwang@snu.ac.kr

Abstract— **In this paper, we introduce a framework to guide decision makers evaluating information security policy performance. It is motivated by lack of adequate decision making mechanism with broader scopes and easy to use for the decision makers. The framework, which adopts Analytic hierarchy Process (AHP) methodology, is developed into a four level hierarchy (goal, criteria, sub-criteria, and alternatives) representing different aspects of information security policy. A survey based on AHP methodology was conducted to obtain decision maker preferences. Instead of relying on dedicated AHP software, we prefer to clearly demonstrate the process of AHP calculations by using Open Office Calc in data analysis. The aims are to show the applicability of open source software in handling AHP decision making problem and to help decision makers in understanding AHP data analysis procedures without relying on proprietary software. Results show that decision makers prefer availability of information security as highest priority, followed by confidentiality and integrity. The findings reflect future strategy in order to improve the effectiveness of information security policy in the organization.**

Index Terms—**information security policy, decision making, Analytic Hierarchy Process, open source.**

I. INTRODUCTION

The Analytical Hierarchy Process (AHP) is a decision support system to deal with multi criteria decision making (MCDM) problems developed by Saaty [1]. It aims to quantify relative priorities for a given set of alternatives on a ratio scale, based on decision maker judgments, by strictly following consistency standard of the pair wise comparison in the decision-making process.

Since a decision-maker bases judgments on knowledge and experience, then makes decisions accordingly, the AHP approach agrees well with the behavior of a decision maker. The strength of this approach is that it organizes tangible and intangible factors in a systematic way, and provides a structured yet relatively simple solution to the decision making problems [2]. In addition, by breaking a problem down in a logical fashion from the large, descending in gradual steps, to the smaller and smaller, one is able to connect, through simple paired comparison judgments, the small to the large. As a result, AHP has been widely adopted in various areas of research and practices these days such as government [18], business management [19] industry [20], health [21], education [22] and many other areas [4]. It mainly used for making selection, evaluation, cost and benefit analysis, resource allocations, planning and development, priority and ranking, and forecasting [23].

This study is proposed with the aim at filling the gap in information security policy literatures particularly from decision making perspectives. While the significance of implementing information security policy has been strongly recommended [7] not only at organizational levels [24] but even recently at national levels [25], there are only few studies on how a decision made with this regard [17].

Studies from academic [6] and professional [26] perspectives show lack of integrated decision making approaches in information security policy since they mostly focuses on technical [5,27] and managerial aspects of security such as ISO 17799, an international standard for information security management [28]. To understand the problem thoroughly, various aspects related to this domain should be studied and thus considered equally in decision making process.

On the grounds of the multi aspects nature of information security policy, we argue that this field is a

* Corresponding author: Irfan Syamsuddin
Based on "Information Security Policy Decision Making: An Analytic Hierarchy Process Approach" by Junseok Hwang and Irfan Syamsuddin which appeared in The Proceedings of 3rd IEEE Asia International Conference on Modelling & Simulation AMS 2009 © IEEE.

doi:10.4304/jsw.5.10.1162-1169

kind of multi criteria decision making (MCDM) problem that can be overcome by using AHP method.

The primary focus of this study lies in the application of AHP through step by step mathematical calculation to solve decision making problem in the specific area of information security policy. Open Office Calc is selected to show details of AHP procedure and to demonstrate the potential of open source software as a powerful tool to solve multi criteria decision making problems.

The organization of this study is structured as follows. Section 2 presents literature review of information security. The next section presents our research objectives and methodology. Then, we introduce our AHP decision model in section 4. It is followed by analysis and discussion in the following. Finally, conclusion and future research direction are given in section 6.

II. Literature Review

Information security is defined as the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources to achieve specified security policy objectives [5]. These laws, rules, and practices must identify criteria for according individuals authority, and may specify conditions under which individuals are permitted to exercise their authority. To be meaningful, these laws, rules, and practices must provide individuals reasonable ability to determine whether their actions violate or comply with the policy [5, 6].

Among various information security and privacy controls, information security policy is considered as a soft approach to deal internally with security related issues to organizations [29]. It is intended to be main reference for organization to safely maintain data, information systems and general electronic base activities [6,29].

Basically, security policy determines technical security measures such as policies applied to firewall, virtual private network VPN and intranet/ internet communications. These policies determine what users may and may not do with respect to security and privacy countermeasures [27].

However, it is no longer the exclusive domain of technical issues [10] as mentioned by Ransbotham and Mitra [30] that many security breaches cases have shown information security has been more a management issue.

The role of information security policy is believed to be more important these days and has broader scope due to increasing cyber threats faced by many organizations [28]. Similarly, Bacik [7] argues that the impacts of information security breaches have been increasingly affecting non technical aspect of organizations such as organizational human resources, finance and stock market. Thus, due to such changes there is strong requirement to reevaluate ISP performance by kindly considering all of related aspects.

In order to accommodate different perspectives found in literature, we propose a classification based on main information security policy aspects as mentioned below.

- *Aspect of Management*. Information security management with standardized security policy is confirmed to become a required tool by many organizations particularly those that rely heavily on the Internet to conduct their operations [8]. Compliance to international standard such as ISO 17799 [28], and implementation of data classification procedures and access control [31] are few examples of emphasis in managing information security. This can be done properly with strong support from top management combined with a commitment by all members of the organization to explicitly prevent the possibility of security risks [9].
- *Aspect of Technology*. Technical side of information security in terms of data, hardware, and applications has become a concern since the beginning of the computer era. This includes terminal security, network security, and Internet security [10]. The significance of technical aspect of information security can be seen from ongoing research in this area such as virus [32], worm [33] and other technical countermeasures [10] from personal computer to the Internet. In short, various security technologies at all levels are still believed as the key elements to combat information security attacks [10].
- *Aspect of Economy*. In [11], Anderson introduces a new economic perspective of information security. Based on his work, the economic of information security has gained a great intention from researchers academic and professional, such as cost and benefits analysis [34] and security investment evaluation [12] to deal with growing information security issues. Filipek [8] affirms that information security has been a serious business priority since many evidences show how cyber attacks have damaged business reputation of many companies in stock market [13].
- *Aspect of Culture*. Compare to previous aspects, information security culture is one that lately received serious attention by practitioners and academies. Lack of inherent security awareness culture was believed as the main source of internal security breaches in some organization [14]. Survey shows a significant amount of cyber security breaches come from internal organization [35]. Schlienger and Teufel [16] justify that information security policy will be effective only if adequate security culture exist within an organization [16]. There are many ways to establish security culture. While Herath and Tao [29] confirm the role of penalties and pressures in establishing security culture, other researchers argue that security education [15] and organizational leadership [9] are paramount.

> Apart from these arguments, security awareness is believed as the core of security culture and it should become inherent responsibility by all members of the organization [16]. An organization with security culture aligns its business objectives with security culture by means that violating security policy is violating business objectives [14].

Although there are various perspectives in viewing information security policy, they are supporting each other and having the same objective of securing information assets from unauthorized parties or illegal actions. Since the early stage of computer security until recent sophisticated internet security management, the purposes of security and privacy controls are unchanged which are to ensure confidentiality, integrity and availability of information and systems [7].

Discussion above also reflects how the importance of information security policy has been widely accepted, promoted and forced in different ways [8]. Unfortunately, only few studies discuss about how decision making done in this specific field [17].

This study was based on a requirement to perform evaluation on information security policy implementation on government institutions with e-government services. Unavailability of widely accepted method to guide decision making is considered as a gap in information security policy literature.

Therefore, we limit our scope in this paper on decision making side of information security policy. We argue that multi criteria decision making (MCDM) can be applied to this study since many aspects are involved and should be considered in balanced to make the best decision among various alternative solutions.

The main contribution this study lies in its in-depth application of AHP as a highly flexible and powerful method as a guidance for those who responsible in making decisions for better implementation of information security policy.

III. Research Objectives and Methodology

A. Research Objectives

Our primary research objective was to develop an empirically grounded model/ framework that would allow information security decision makers to make decision regarding information security policy issues.

Given the fact that most AHP base decision making papers apply specific proprietary AHP software such as Expert Choice and HIPRE, in this study we propose a different way by illustrating AHP calculations procedure using open source software. Our choice goes to Open Office Calc, open source spreadsheet software commonly available in various Linux packages. By doing so, we extend our study to achieve two additional objectives as follows:

Firstly, it is intended to shows the applicability of open source software a suitable and easy tool in performing step by step of AHP calculations. Furthermore, this study provides strong basis for further development of open source AHP application.

Secondly, through an example of AHP calculation this study will benefit decision makers involved in this study and also wider readers to understand AHP calculation processes. Although it seems more difficult than by using dedicated AHP software, our attempt will benefit those who want to learn AHP in more detail.

.

B. Methodology

We prefer for our study to use the Analytic Hierarchy Process (AHP) because it has been a widely accepted and applied to solve numerous multiple criteria decision making problems in different contexts [4] during the last twenty five years or more [23].

Within its framework, a decision problem (usually a complex one) is decomposed into a hierarchy of the goal, criteria, sub-criteria, and finally the alternatives lying at the bottom of the hierarchy.

Saaty [1] explains the following four main characteristics of AHP:

- based on multiple attribute hierarchies
- assessing weights by a pairwise comparison of attributes
- assessing preferences by a pairwise comparison of alternatives
- consistency analysis

Zahedi [4] describes these characteristics into a four steps of AHP calculation procedure as follows:

Step 1. Develop the hierarchy

This consists of decomposition of the problem into elements based to its characteristics and the formation. Basically, a hierarchy consists of goal, criteria and alternatives and can be expanded depends on requirements.

Step 2. Comparing and obtaining the judgment matrix.

In this step, the elements of a particular level are compared with respect to a specific element in the immediate upper level. The resulting weights of the elements may be called the local weights.

TABLE I
PAIR WISE COMPARISON MATRIX A

	M	**T**	**E**	**C**
Management (M	1	4	4	3
Technology (T)	1/4	1	2	1/2
Economy (E)	1/4	½	1	1/6
Culture (C)	1/3	2	6	1

The matrix A can be defined by

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

where *n* is the order of matrix.

Then the consistency property in the pair wise comparison is examined by a two steps procedure as follows [1]:

- Develop the normalized pariwise comparison matrix A_1

$$A_1 = \begin{bmatrix} a'_{11} & a'_{12} & \cdots & a'_{1n} \\ a'_{21} & a'_{22} & \cdots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{n1} & a'_{n2} & \cdots & a'_{nn} \end{bmatrix}$$

and $a_{ij} = \dfrac{a_{ij}}{\sum_{i=1}^{n} a_{ij}}$ for i , j = 1, 2,…, n.

- Test the consistency property.

Where CI is the consistency index, CR is the consistency ratio, λ_{max} is the largest eigenvalue of the pair wise comparison matrix, n is the matrix order, and RI is random index. Table 3 shows a set of recommended RI values presented by Saaty [1].

TABLE II
RANDOM INDEX

N	**1**	**2**	**3**	**4**	**5**
RI	*0*	*0*	*0.52*	*0.89*	*1.11*

N	**6**	**7**	**8**	**9**	**10**
RI	*1.25*	*1.35*	*1.40*	*1.45*	*1.49*

This is argued as one of AHP's advantages which able to measure whether or not inconsistency occurs in the judgment process. If CR values are > 0.10 for a matrix larger than 4x4, it indicates an inconsistent judgment. In some parts decision makers should revise the original values in the pair wise comparison matrix until desired consistency level reached.

Step 3: Local weights and consistency of comparisons.

In this step, local weights of the elements are calculated from the judgment matrices using the eigenvector method (EVM). The normalized eigenvector corresponding to the principal eigenvalue of the judgment matrix provides the weights of the corresponding elements.

$$W = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}, \text{ and } \quad w_i = \frac{\sum_{i=1}^{n} a'_{ij}}{n} \quad \text{for i = 1, 2,…, n}$$

Then W' is obtained as a new matrix based on multiplication between matrix A and W as described below

$$W' = A.W = \begin{bmatrix} w'_1 \\ w'_2 \\ \vdots \\ w'_n \end{bmatrix}$$

and $\lambda_{\max} = \dfrac{1}{n}\left(\dfrac{w'_1}{w_1} + \dfrac{w'_2}{w_2} + \cdots + \dfrac{w'_n}{w_n}\right)$

Where W' is the eigenvector, w_i is the eigenvalue of criterion I, and λmax is the largest eigenvalue of the pair wise comparison matrix.

Step 4: Aggregation of weights across various levels to obtain the final weights of alternatives.

This final step of AHP procedure where the local weights of elements of different levels are aggregated to obtain final weights of the decision alternatives (elements at the lowest level).

IV. AHP DECISION MODEL

In this section, the development of AHP decision model for information securoty policy is explained. We construct the hierarchy for information security policy decision making that combines multi criteria, different aspects and alternatives. It adopts AHP which enables structuring, measurement and synthesizing of decision hierarchy [1] to make good decisions.

Figure 1 shows the structure of our AHP decision model. It is a four layer hierarchy consists of goal, criteria, sub-criteria and alternatives. All layers are described as follows.

First of all, the first layer defines the goal to be achieved, in this case information security policy decision.

Secondly, the next layer consists of four criteria. These criteria are based upon the classification in literature review namely, management (M), technology (T), economy (E) and culture (C).

Thirdly, we specify the four main criteria into several sub-criteria. There are ten sub-criteria as can be seen in table 3.

Finally, at the last layer of the hierarchy, triangle security objectives (confidentiality, integrity and availability) are set as alternatives.

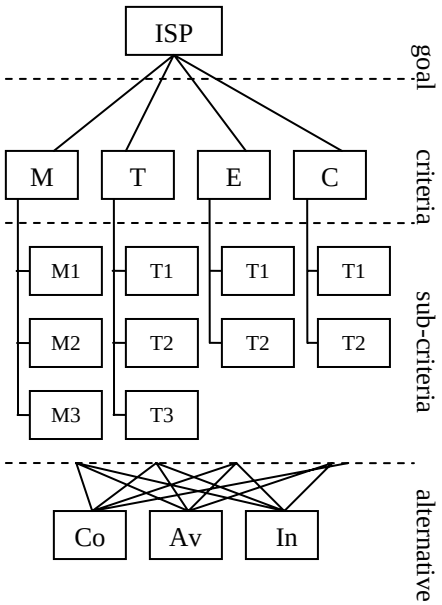


Figure 1. AHP Hierarchy.

TABLE III
CRITERIA AND SUB CRITERIA

Criteria	Sub Criteria
Management (M)	Comply with standard (M1) Regular Review (M2) Commitment (M3)
Technology (T)	End point security (T1) Network security (T2) Application security (T3)
Economy (E)	Security Investment (E1) Cost of Attack (E2)
Culture (C)	Reward & Punishment (C1) Security Education (C3)

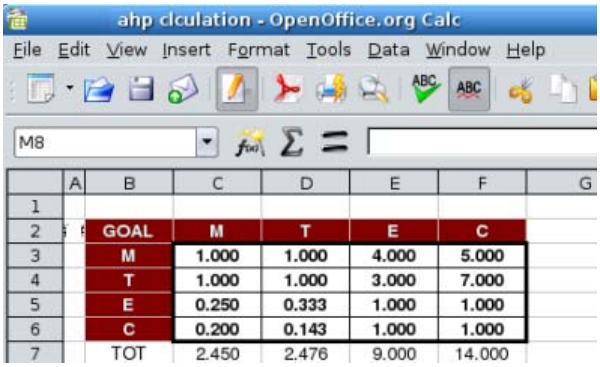
Accordingly, AHP based survey [1][17] was created and distributed to chief information officers of government institution which maintain e-government services as intended audiences in this study [17]. Subsequently, further analysis and discussion are given in the following section.

V. AHP ANALYSIS AND DISCUSSION

In this paper, we prefer to perform step by step of AHP calculation manually instead of relying on dedicated AHP software. For this purpose, we choose Open Office Calc, an open source equivalent to Microsoft Excel to illustrate AHP calculations. Our AHP experiment was run under Linux Mepis Live-CD.

Figure 2 shows the pair wise comparison values of four criteria with respect to goal in Open Office Calc spreadsheet. For example, cell F3 (5.000) represents pair wise comparison value between criteria Management and Culture and so forth.

The next step is to define eigenvalue. The eigenvalue is obtained by performing two steps. First, each pair wise value is divided by the total of corresponding column; this will generate normalized values in the same matrix structure. Second, the average of normalized values in each raw is calculated which represents eigenvalue.



	A	B	C	D	E	F	G
1							
2		GOAL	M	T	E	C	
3		M	1.000	1.000	4.000	5.000	
4		T	1.000	1.000	3.000	7.000	
5		E	0.250	0.333	1.000	1.000	
6		C	0.200	0.143	1.000	1.000	
7		TOT	2.450	2.476	9.000	14.000	

Figure 2. AHP pair wise comparison for goal.

The entire pair wise comparisons and corresponding eigenvalues are represented in figure 3. For instance, the eigenvalue for the management, technology, economy and culture criteria are 0.403, 0.411, 0.105 and 0.80 respectively.

The following steps describe how the calculations were performed in Open Office Calc as shown in figure 3 above:

- Calculate total column of first matrix. Here, we obtained 2.45 in cell C7 as the total of C3,C4,C5 and C6.
- Create new matrix with normalized values. The normalized value for cell I3 (M-M) was obtained by dividing its original pair wise value (cell C3) with the total column M (C7).
- The same calculations were performed for the remaining cells until the complete new matrix generated.
- Eigenvalue was calculated as the average value of each row of the new matrix. For example, eigenvalue for management criteria was the average value of row 3 ((0.408+0.404+0.444+ 0.357)/4).
- Perform the similar calculation processes for all matrixes.

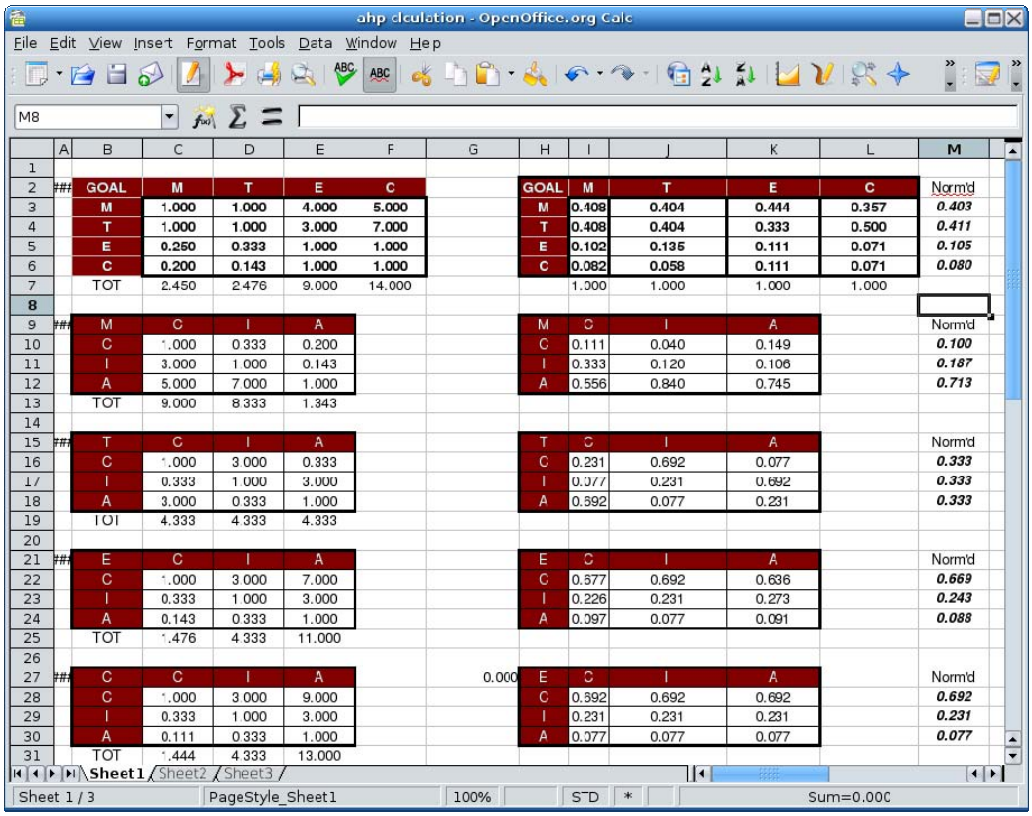


Figure 3. Matrix of pair wise comparisons

The next step was to calculate the overall priority of alternatives with respect to criteria. Based on eigenvalues obtained in previous steps, we developed two matrixes in order to ease further calculations in the next steps.

The first matrix was for the upper level eigenvalue of criteria with respect to goal. The second matrix was for lower level eigenvalue of alternative with respect to criteria. Both matrixes can be seen in figure 4.

As can be seen the values of first level matrix from cell J34 to J37 are 0.403, 0.411, 0.105 and 0.080 in that order. These numbers were actually the eigenvalues copied from cell M3 to M6.

In terms of the second level matrix, the values were also taken from eigenvalues for each alternative with respect to four criteria (see figure 4). For example, the values of cell D35 to D37 were eigenvalues of the three alternatives with respect to management criteria. The numbers were then copied from cell M10 to M12 (0.100, 0.187, and 0.713).

The similar processes were performed for column E (technology), column F (economy), and column G (culture) from row 35 to row 37 which represent the eigenvalues of confidentiality, integrity and availability with respect to these criteria. Column E (from E35 to E37) contains 0.333, 0.333, and 0.333; column F (from F35 to F37) contains 0.669, 0.243, and 0.088; and column G (from G35 to G37) contains 0.692, 0.231, and 0.077. Two matrixes were generated.

Then we move to the last step to obtain overall priorities. It was done by matrix multiplication between both matrixes. For example, in order to obtain overall priority for confidentiality (cell D39), the following calculation was performed

$$= (D35*J34) + (E35*J35) + (F35*J36) + (G35*J37)$$

The result was 0.303 for confidentiality. In other way, this process can be simplified by using MMULT function [3]. It is a built in function in Open Office Calc to perform automatic matrix calculation, in this case between second level matrix (D35:G37) and first level matrix (J34:J37). The function was expressed as

=MMULT(D35:G37,J34:J37).

Finally, we obtained the final result as can be seen in figure 4. The first rank goes to availability with the highest value of 0.440, followed by confidentiality and integrity as the second and third ranks which accounted for 0.303 and 0.256 respectively (see table 4).

TABLE IV
OVERALL PRIORITY RESULT

Confidentiality	0.303
Integrity	0.256
Availability	0.404

Based on the overall priority result, it is clearly found that decision makers consider the importance of availability of the information and the systems as the

highest portion to be improved in terms of information security policy. The second and the last priorities preferred by decision makers are confidentiality and integrity do not that both are not important at all. This means the portion of confidentiality and integrity considerations by the decision makers will be lesser than availability for the purpose of information security policy improvement.

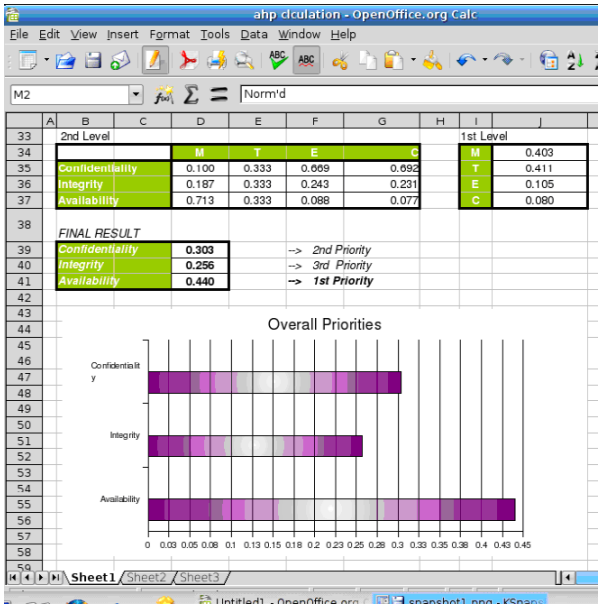


Figure 4. Overall priority

Information security is a growing field which always provides more spaces for innovation. Threats on information assets will keep being serious security issues in the future. Types of security attacks and scope of its impacts might be different depend on different circumstances. Therefore re-evaluation of security countermeasures such as information security policy is strongly required to adapt with such changes.

Decision making framework proposed in this study with example of AHP calculation will be a valuable tool for those who responsible to make decision in this field.

VI. Conclusion and Further Research

The main practical implication of this study is the application of AHP method to guide information security policy decision making. Moreover, the research contributes information security policy literatures with a new empirical case from decision maker point of view.

Based on the results, governments' chief information officers are recommended to give more attention to enhance the availability of information in the future since it accounted for the highest decision preference value, followed by confidentiality and integrity. The results may be different according to the type of organization and security threats they face.

The example of AHP analysis with Open Office Calc shows the applicability of open source software as powerful tool for decision making purposes. In addition, this approach also contributes from educational perspective, in providing an easy to follow example on how to make decision without depending on dedicated AHP software.

This study provides a foundation for further research, to build open source AHP software with adaptable capabilities regardless of the number of hierarchy levels.

Acknowledgement

The authors would like to great thank the editor in-chief, Prof. Dr. Kassem Saleh, and the anonymous referees for their constructive comments and suggestions that led to an improved version of this paper.

References

[1] T.L. Saaty, *The Analytic Hierarchy Process*, RWS Publications, Pittsburgh, PA. 1990.

[2] B.L. Golden, E.A. Wasil, and P.T. Harker, *The Analytic Hierarchy Process: Applications and Studies*. New York, NY: Springer-Verlag, 1989.

[3] Open Office, available at http://www.openoffice.org (accessed 2 December 2009).

[4] F. Zahedi, "The analytic hierarchy process—a survey of the method and its applications", *Interfaces*, vol.16, no. 4, pp. 96–108, 1986.

[5] D.F. Sterne, "On the Buzzword 'Security Policy,'" *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, California, pp. 219-230, 1991.

[6] W.E. Kuhnhauser and M.K. Ostrowski, "A Formal Framework to Support Multiple Security Policies," *Proc. 7th Canadian Computer Security Symposium.* Ottawa, Communication Security Establishment Press, pp. 1-19. 1995.

[7] S. Bacik, "Building an effective information security policy architecture", CRC Press. LLC, Boca Raton, 2008.

[8] R. Filipek, "Information security becomes a business priority", *Internal Auditor*, vol. 64, no.1, pp.18, 2007.

[9] O. Zakaria, "Information Security Culture and Leadership", *Proceedings of the 4th European Conference on Information Warfare and Security*, Cardiff, Wales, pp 415-420, 2005.

[10] A. Householder, K. Houle, and C. Dougherty, "Computer attack trends challenge Internet security", *Computer IEEE*, vol. 35, no. 4, pp. 5-7, 2002.

[11] R. Anderson, "Why Information Security is Hard : An Economic Perspective", *Proceedings of 17th Annual Computer Security Applications Conference*, pp. 10-14, 2001.

[12] L.A. Gordon and M. P. Loeb, "The Economics of Investment in Information Security", *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457, 2002.

[13] S.E. Schecter and D.S. Michael, "How much security is enough to stop a thief ? The economics of outsider theft via computer systems networks", *Proceedings of theFinancial Cryptography Conference*, Guadeloupe. pp. 122-137, 2003.

[14] A. Martins and J. Eloff , "Information security culture", *IFIP TC11, 17th international conference on information security (SEC2002)*, Cairo, Egypt, pp. 203–214, 2002.

[15] M.E. Thomson and R. von Solms, "Information security awareness: educating your users effectively", *Information*

Management and Computer Security, vol. 6, no. 4, pp. 167–173, 1998.
[16] T. Schlienger and S. Teufel, "Information Security Culture: The Socio-Cultural Dimension in Information Security Management", *Proceedings of the IFIP TC11 17th International Conference on Information Security*, pp. 191 – 202, 2002.
[17] J. Hwang and I. Syamsuddin, "Information Security Policy Decision Making: An Analytic Hierarchy Process Approach", *Proceeding of IEEE 2009 Third Asia International Conference on Modelling & Simulation*, pp. 158-163, 2009.
[18] Kahraman, Cengiz, Demirel, N. Cetin, Demirel and Tufan, "Prioritization of e-Government strategies using a SWOT-AHP analysis: the case of Turkey", *European Journal of Information Systems*, vol. 16, no. 3, pp. 284-298, 2007.
[19] M.C. Lin, C.C. Wang, M.S. Chen and C.A. Chang, Using AHP and TOPSIS approaches in customer-driven product design process, *Computers in Industry* , vol. 59, no. 1, pp. 17–31, 2008.
[20] C.Unal and G.G. Mucella, "Selection of ERP suppliers using AHP tools in the clothing industry", *International Journal of Clothing Science and Technology*, vol. 21, no. 4, pp. 239-251, 2009.
[21] L.A. Vidal, E. Sahin, N. Martelli, M. Berhoune and B. Bonan, "Applying AHP to select drugs to be produced by anticipation in a chemotherapy compounding unit", *Expert Systems with Applications*, vol. 37, no. 2, pp. 1528-1534, 2010.
[22] W. Ho, H.E. Higson, P.K. Dey, X. Xu and R. Bahsoon, "Measuring performance of virtual learning environment system in higher education", *Quality Assurance in Education* , vol.17, no. 1, pp. 6-29, 2009.
[23] O.S. Vaidya and S. Kumar, "Analytic hierarchy process: An overview of applications", *European Journal of Operational Research*, vol. 169, no. 1, pp. 1–29, 2006.
[24] H. Fulford and N.F.Doherty, "The application of information security policies in large UK-based organizations: an exploratory investigation", *Information Management & Computer Security*, vol. 11, no. 3, pp. 106 – 114, 2003.
[25] C.Y. Ku, Y.W. Chang and D.C. Yen, "National information security policy and its implementation: A case study in Taiwan", *Telecommunications Policy*, vol. 33 , no. 7, pp. 371-384, 2009.
[26] K. Shannon, P. Anne, H. Ben, P. Chad and C. Matt, "Information security threats and practices in small businesses", *Information Systems Management*, vol. 22, no 2 pp. 7-19, 2005.
[27] A.Herzog and N. Shahmehri, "Usable Set-up of Runtime Security Policies", *Information Management & Computer Security*, vol. 15, no. 5, pp 394-407, 2007.
[28] M.C. Lee and T. Chang, "Applying ISO 17799:2005 in information security management", *International Journal of Services and Standards*, vol. 3, no. 3, pp.352 – 373, 2007.
[29] T. Herath and H.R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, vol. 47, no. 2, pp. 154-165, 2009.
[30] S. Ransbotham and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information Systems Research*, vol. 20, no. 1, pp. 121-139, 2009.
[31] C. Huang, J. Sun, X. Wang and Y.J. Si, "Security Policy Management for Systems Employing Role Based Access Control Model", *Information Technology Journal*, vol. 8, no. 5, pp. 726-734, 2009.
[32] C. Jin, J. Liu, and Q. Deng, "Network Virus Propagation Model Based on Effects of Removing Time and User Vigilance", *International Journal of Network Security*, vol. 9, no. 2, pp. 156-163, 2009.
[33] T. Komninos, P. Spirakis, Y.C. Stamatiou, G. Vavitsas, "A Worm Propagation Model based on Scale Free Network Structures and People's Email Acquaintance Profiles", *International Journal of Computer Science and Network Security*, vol. 7, no. 2, pp. 308-315, 2007.
[34] S.A. Butler, "Security attribute evaluation method: a cost-benefit approach", *Proceedings of the 24th International Conference on Software Engineering*, pp. 232-240, 2002.
[35] Verizon, "Data Breach Investigations Report 2009", available at: http://www.verizonbusiness.com (accessed 22 February 2010).

Irfan Syamsuddin is a lecturer at State Polytechnic of Ujung Pandang, Makassar, Indonesia. Currently he is pursuing PhD research at International Information Technology Policy Program (ITPP), Seoul National University Republic of Korea. Previously, he obtained B.Eng degree in Electrical Engineering from Hasanuddin University, Indonesia, then received his Postgraduate Diploma in Business Electronic Commerce and Master of Commerce in Internet Security Management degrees both from Curtin University of Technology, Perth, Australia.

Prof. Junseok Hwang is a US-trained Engineer and currently serving as a Director and Dean of the Technology Management, Economics and Policy Program (TEMEP) and of the International Information Technology Policy Program (ITPP) at the Seoul National University and Associate Professor at the Seoul National University Republic of Korea.Dr. Hwang received his B.S. degree from Yonsei University, Korea specializing in Mathematics, his M.S. degree in Telecommunications from the Univ. of Colorado, and his Ph.D. in Information Science and Telecommunications from the University of Pittsburgh, Pittsburgh, PA in the United States.