The Application of AHP to Evaluate Information Security Policy Decision Making

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

Junseok Hwang
[1] International IT Policy Program (ITPP)
TEMEP, College of Engineering
Seoul National University
Seoul, Republic of Korea
e-mail: junhwang@snu.ac.kr

***Abstract*—This paper examines the application of AHP in evaluating information security policy decision making with respect to Indonesian e-government systems. We suggest a new model based on four aspects of information security (management, technology, economy and culture) and three information security components (confidentiality, integrity and availability). AHP methodology was applied to analyze the decision making process. It is found that management and technology were the dominant aspects of information security, while availability was the main concern of information security elements for e-government information systems.**

Keywords: AHP; information security; policy; decision making

I. INTRODUCTION

Decision making is considered as one of the challenging task in human life. The difficulties will arise when there are many aspects to be considered equally at the same time with respect to make the best decision that satisfy all stakeholders.

In the era of information, the existence of policy for specifically guiding information security approaches within organization is urgently needed. However, in order to develop effective information security policy, different aspects should be considered appropriately. Literature review shows how information security developments were dominated mainly by technical and managerial aspects as mentioned by Anderson [1]. On the other hand, sophisticated information technology has been deeply affecting economic and cultural aspect of today’s information society. Therefore, integrating economic and cultural insights into information security related decisions should be considered in order to gain more benefits from different perspectives. Therefore, an adequate method to allow careful analysis by incorporating those aspects of information security aspects is highly required.

This paper aimed at examining the application of Analytic Hierarchy Process (AHP) as a method to support information security decision making with the case of Indonesian e-government systems.

In the following section, we describe several related aspects and components of information security applied in this study. Then, AHP based evaluation model is introduced in section 3. The result and analysis are discussed in the following section. Finally, conclusion and future research directions are given in section 5.

II. INFORMATION SECURITY ASPECTS AND COMPONENTS

In this section, we briefly describe important aspects and components of information security policy. Dhillon and Blackhouse [2] define information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The role of information security has become more important since many people, business, and government institutions store, process and maintain their data in digital format and share them using various types of information technology. In such dynamic environment, security plays a significant role and should be put into the first consideration. It is argued by Filipek [3] that information security policy should become business priority as it has significant role to guarantee trust in digital age.

Conforming to the information security policy is strongly recommended in order to make organizations aware and well prepared for growing cyber security threats in various forms in the future.

Information security related literatures show various matters attributed to information security policy. Therefore, we classify them into main aspects and components of information security policy as follows.

A. Information Security Aspects

- **Management.** Management aspect of information security has been realized as essential in ensuring information handling within organization. Filipek [3] states that it covers data classification, access control, etc.
- **Technology.** Securing information technology in terms of data, hardware, and applications has been the most concerned aspect since the beginning of computerized era. It includes computer security, wired and wireless network security and internet security [4].
- **Economy.** Previously, this aspect was seen only as an object of information security issues. However, recently it has been proven that economic considerations play a significant role in ensuring the level of security measures within an organization [1]. Without considering different aspects of economy involving in information security, such as incentives, investment and information sharing (particularly financial information), one will not be able to determine economic benefit of such protections as argued by Gordon and Loeb [5]. Through economic aspect, measurements of information security can be done quantitatively as suggested by Schecter and Michael [6].
- **Culture.** Among other aspects, cultural view is the least aspect concerned by experts The role of culture in maintaining security should not be under estimated since security breaches often caused by inadequate behaviors from internal organization [7]. Therefore, internal security approaches are encouraged in the form of security awareness. It is affirmed by Thomson and von Solms [8] that combination of security education and organizational leadership is the critical success factor for an organization to effectively promote security awareness and gradually develop a security culture within an organization.

B. Information Security Components

Confidentiality, integrity and availability (known as CIA Triad) are three traditional components of information security widely accepted in information security literatures [2-4],. It is often called security triad which should be fulfilled appropriately in order to achieve security objectives within an organization.

- **Confidentiality.** Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Confidentiality reflects protection of the privacy users in respect to their own information.
- **Integrity.** It means that data cannot be modified without authorization. Integrity ensures that only authorized user able to access the data.
- **Availability.** It means that for any information system to serve its purpose, the information must be available when it is needed. Availability ensures the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

III. Information Security Policy Model

With the aim to make the evaluation of information security policy, we propose a new model as can be seen in figure 1. The evaluation model is constructed into a three level hierarchy which items are derived from previous literature study. On top level we specify the objective of our study which is information security policy evaluation followed by four main aspects of information security policy and the three security components arranged on the second and third levels.

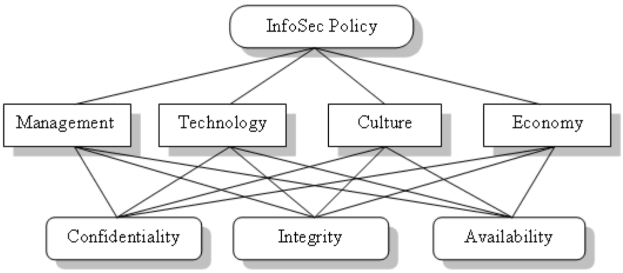


Figure 1. Proposed information security policy evaluation model.

A. Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) is a multi criteria decision analysis proposed by Saaty [9]. AHP is preferred in this study since it aligns with our classification and hierarchical approaches represented in our model. Additionally, AHP has been proven as the most widely used technique of multi-criteria decision making during the last twenty five years or more [10].

With AHP, a complex decision problem (with tangible and intangible factors) can be developed properly. Further, decision makers may perform both qualitative and quantitative analysis simultaneously with this technique.

In general, AHP can be easily applied in four simple steps below [11]:

Step 1. Structure the problem into hierarchy.

This consists of decomposition of the problem into elements based to its characteristics and the formation. As can be seen in figure 1, the model consists of three levels (goal, criteria and alternatives).

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.

Step 3: Local weights and consistency of comparisons.

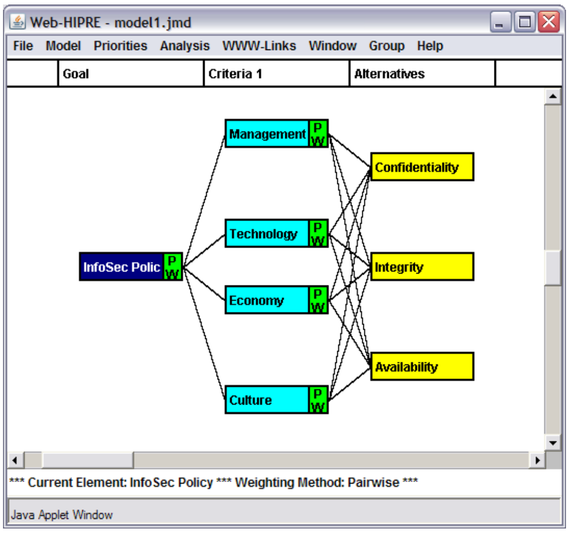
Here, local weights of the elements are calculated from the judgment matrices using the eigenvector method (EVM).

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

In this final step, the local weights of elements of different levels are aggregated to obtain final weights of the decision alternatives (elements at the lowest level).

B. AHP Analisis

AHP analysis was done with Web-HIPRE. It is a multi criteria decision support system which provides a set of analytical methods such as SMART, SMARTER, as well as AHP. In addition to various decision analysis methods, another benefit of Web-HIPRE is its freely available online which allows the use of this program more widely. Furthermore, it also supports AHP group decision analysis to gain aggregate of several decision makers into single decision [12]. Figure 2 shows our evaluation model developed in Web-HIPRE.



*** Current Element: InfoSec Policy *** Weighting Method: Pairwise ***

Figure 2. The AHP Evaluation model in Web-HIPRE.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

IV. Results and Discussion

One of the advantages of AHP is its ability 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 as mentioned by Saaty [9]. It is sometimes difficult and time consuming tasks to ask decision makers repeat the survey. However, this should be done in order to keep the level of inconsistency measure at acceptable limit and to justify the final results.

Based on survey, we fulfilled paired comparison matrix online. At this stage, we created five comparison matrices which represent decision maker opinion of recent information security policy implementations according to the evaluation model.

TABLE I. Pairwise Comparison of Criteria

A: Comparison of criteria with respect to the Goal					
	M	T	E	C	Local Weight
M	1.0	1.0	4.0	5.0	0.401
T	1.0	1.0	3.0	7.0	0.415
E	0.25	0.33	1.0	1.0	0.104
C	0.2	0.14	1.0	1.0	0.080
Consistency Measure					0.127

Table 1 shows comparison matrix of criteria with respect to the goal. It is clearly revealed that technical and management aspects are still dominating the portion of overall information security policy perspectives which accounted for 0.114 and 0.401 of local weight, followed by economic and cultural aspects of 0.104 and 0.080 respectively. It is important to note that priority of security criterion here might reflects the specific environment and it can be vary depends on different environments.

TABLE II. Pairwise Comparison of Alternatives

B: Comparison of Alternatives with respect to Management				
	C	I	A	Local Weight
C	1.0	0.33	5.0	0.279
I	3.0	1.0	7.0	0.649
A	0.2	0.14	1.0	0.072
Consistency Measure				0.121

C: Comparison of Alternatives with respect to Technology				
	C	I	A	Local Weight
C	1.0	0.11	0.2	0.062
I	9.0	1.0	3.2	0.680
A	5.0	0.31	1.0	0.257
Consistency Measure				0.085

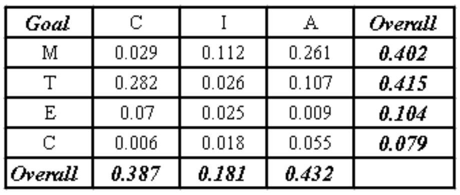
D: Comparison of Alternatives with respect to Economy				
	C	I	A	Local Weight
C	1.0	3.0	7.0	0.669
I	0.33	1.0	3.0	0.243
A	0.14	0.33	1.0	0.088
Consistency Measure				0.042

E: Comparison of Alternatives with respect to Culture				
	C	I	A	Local Weight
C	1.0	3.0	9.0	0.692
I	0.33	1.0	3.0	0.231
A	0.11	0.33	1.0	0.077
Consistency Measure				0.000

Similarly, Table II.(B, C, D and E) represent local weight of all three alternatives (confidentiality, integrity, and availability) with respect to individual criteria. In terms of consistency, it is important to note that although both matrices (table 1 and II.B) show a little inconsistency measures (0.127 and 0.121), they are acceptable since the overall consistency measure is less than maximum point [9][12].

Then, the last step was performed to obtain global weight value or composite overall priorities as a final weight of alternatives. The final result is represented in table 3 below.

TABLE III. FINAL RESULT



Goal	C	I	A	*Overall*
M	0.029	0.112	0.261	***0.402***
T	0.282	0.026	0.107	***0.415***
E	0.07	0.025	0.009	***0.104***
C	0.006	0.018	0.055	***0.079***
Overall	***0.387***	***0.181***	***0.432***	

Based on these results, we discuss the main findings as follows. In terms of security alternatives, availability is regarded as the highest priority by decision maker compare to confidentiality and integrity. It is found that availability has accounted for 0.432, whilst confidentiality and integrity have accounted for 0.387 and 0.181 respectively.

Similarly, it is found that technology and management are considered to be more important than economic and cultural aspects. Government seems to put more concern on management and technological aspects of information security which accounted for 0.415 and 0.402 respectively compare to economy and cultural concerns which only 0.104 and 0.079 respectively.

This finding reflects imbalanced approach of information security policy development in government sector. Whereas, in order to be effectively applied, cultural insights [7,8] as well as economic perspectives [3,5,6] should also obtain more concerns in shaping a sound and effective information security policy implementations. Thus, we confirm that these findings has shown supporting evidence to our previous study in [13], which pointed out information security as one of the challenging issues to develop effective e-government systems in Indonesia.

Through the application of AHP in this study, we could clearly evaluate the performance of information security policy in both qualitative and quantitative ways. Furthermore, it leads us to propose the following recommendations for better implementation in the future:

- Improve security awareness among government employees by adequate education and training to achieve sound security culture in government environment.
- Economic aspect of information security should be clearly understood and addressed as one of important factors for Indonesian government in recent information era.
- Data integrity should be considered in balance with data availability and data confidentiality, particularly in the case of information exchange or data sharing among government agencies.
- Periodically review the performance of information security policy implementations using the AHP model proposed in this study.

V. CONCLUSION

This study justifies the application of AHP method to solve information security evaluation. AHP provides a robust and encompassing treatment for decision makers in both qualitative and quantitative ways as found in this study.

We have shown how AHP model might be used to assist decision maker evaluate information security policy implementation. From the perspective of information security aspect, management and technology aspects are found to be the highest concerns compare to economic and cultural aspects. Similarly, with respect to information security component, availability represents the highest priority in e-government systems followed by confidentiality and integrity.

The main recommendation derived from this study is the promotion of information security awareness through security education and organizational leadership. For further study, we would like to expand it other group of respondents such as industry and university. Through this approach, comparative studies might be conducted to analyze similarities or differences among different groups. Another possible study is the application of ANP (Analytic Network Process) to observe this model from different side.

ACKNOWLEDGMENT

The authors would like to thank the editor in-chief, Professor Emeritus, David Al-Dabass and the anonymous referees for their constructive comments and suggestions that led to an improved version of this paper.

REFERENCES

[1] R. Anderson, “Why Information Security is Hard : An Economic Perspective,” Proc. of 17th Annual Computer Security Applications Conference, 2001, pp. 10-14.

[2] G. Dhillon and J. Blackhouse, “Current directions in IS security research: towards socio-organizational perspectives”, Information Systems Journal, vol. 11, no.2, 2001, pp.127-53.

[3] R. Filipek, “Information security becomes a business priority,” Internal Auditor, vol. 64, no.1, 2007, pp.18.

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

[5] 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, 2002, pp. 438-457.

[6] 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 the Financial Cryptography Conference, Guadeloupe. 2003, pp. 122-137.

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

[8] M.E. Thomson and R. von Solms, “Information security awareness: educating your users effectively,” Information Management and Computer Security, vol. 6, no. 4, 1998, pp. 167–173.

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

[10] O.S. Vaidya and S. Kumar, “Analytic hierarchy process: An overview of applications”, *European Journal of* Operational Research, vol. 169, no. 1, 2006, pp. 1–29.

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

[12] J. Mustajoki and R.P. Hämäläinen, “Web-HIPRE: Global decision support by value tree and AHP analysis,” INFOR, vol. 38, no. 3, 2000, pp. 208-220.

[13] I. Syamsuddin and J. Hwang, “Failure of E-Government Implementation: A Case Study of South Sulawesi," Proc. of IEEE ICCIT Third International Conference on Convergence and Hybrid Information Technology ICCIT, vol. 2, 2008, pp.952-960.