Information Security Policy Decision Making: An Analytic Hierarchy Process Approach

Junseok Hwang[a] , Irfan Syamsuddin[a,b]
[a]*International IT Policy Program*
Seoul National University, Republic of Korea
[b]*State Polytechnic of Ujung Pandang, Republic of Indonesia*
junhwang@snu.ac.kr, irfans@temep.snu.ac.kr

Abstract

This paper addresses the use of a specific decision support methodology in operational research termed the Analytic Hierarchy Process (AHP). We examine the application of AHP method in guiding information security policy decision making with respect to Indonesia. We suggest four aspects of information security policy, namely management, technology, economy and culture. In addition, information security components derived from literature review are applied which are confidentiality, integrity and availability.

Based on information security policy aspects and information security components we introduce our AHP based model of government information security policy. Our examination of this model shows how AHP can help policy makers to produce appropriate decisions. It is found that AHP shows a robust and encompassing treatment useful for decision makers in both qualitative and quantitative ways. Therefore, it is reasonable to apply AHP for larger scope of research.

Keywords : *information security, policy, decision making, AHP*.

1. Introduction

Policy making is considered as the most challenging process in any field. Since many aspects should be considered in balance in respect to produce the appropriate decision for dealing with actual situation as well future planning.

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 [11]. On the other hand, sophisticated information technology has been deeply affected economic and cultural aspect in modern society. Therefore, integrating economic and cultural insights into information security related considerations will also bring valuable benefits. Therefore, a careful analysis incorporating the four aspects with information security aspects is required.

This paper aimed at examining the application of Analytic Hierarchy Process (AHP) as a method to develop information security decision model for future information security policy in Indonesia

The following part (section 2) contains the literature review as the basis of the study. In section 3, we deeply explore several aspects and components of information security. Then, in section 4, we introduce the model based on AHP approach, followed by result analysis and discussion of the findings in section 5. Finally, conclusion and future research directions are given in section 6.

2. Literature Review

Information security policy is one of the fields where decision makers always face a dynamic and multi aspects problems associated with emerging cyber security threats. Although there have been many attempts to secure it, the number of security incidents still significant year by year, particularly when we look at the amount of money loss due to cyber crimes [30][34]. There are some obstacles we found from literature review that contribute to the situation.

Firstly, there are many technologies and standards proposed to secure information systems. Intrusion detection systems, anti viruses and firewalls are few of such technologies which often come with new version that need regular updates from users' side. This point is usually the weakest point where government agencies could not cope with.

Secondly, there are several information technology related standards such as COBIT, ITIL, Octave and

978-0-7695-3648-4/09 $25.00 © 2009 IEEE
DOI 10.1109/AMS.2009.49

ISO 27001 available to IT governance systems as well performing information systems audit. Unfortunately, to implement such standards is mainly affordable only by large business organizations [33].

Lastly, information security policy has not been considered as a vital point by many government organizations in the world. While well developed countries have adequate concerns and actions about information security policy, developing countries are still lag behind [12].

This study intends to propose a model for government information security policy with respect to several aspects combined with information security elements. It is believed that this study will significantly contribute to the current e-government problems by Indonesia as mentioned by Hwang and Syamsuddin [12]. It is affirmed that lack of information related policy is one of the reasons why e-government application was failed in Indonesia [12]. These findings align with the latest UN report [13] which shows the dramatic decrease of Indonesia e-government ranking in the world from 70 in 2003 dropped to 106 in 2008.

Understanding the level of information security awareness in Indonesian government agencies is another objective of this study. For this reason, AHP based survey is given to respondents from several government ministries who at middle management level officials.

3. Information Security Policy Aspects and Components

3.1. Information Security Aspects

In [18], information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction." The role of information security has been realized to become more and more important since many people, business, and government institutions store their data in digital format and share them using various type of information technology.

Security breaches, data stolen, and financial losses announced regularly in several publications [30][34] are few of many cases which reflect the importance of information security policy. Information security policy is developed and applied in response to these growing problems.

In respect to information security policy, instead of the two main aspects (management and technology), we also found that economy and culture are other significant aspects to be considered in formulating information security policy.

The following part describes the four aspects of information security policy applied in this study.

3.1.1. Management. In [15] information security management is confirmed has become a required function by many modern organizations that rely heavily on the Internet to conduct their operations. Even, in many cases, as confirmed in [17], it is too risky to run a business without appropriate assurance for the security of its information systems operations.

3.1.2. Technology. Securing information technology in terms of data, hardware, and applications has been the most concerned aspect since the beginning of computerized era. It covers computer security [25], wired and wireless network security [20][23], and internet security [21]. There have been tremendous efforts to secure information illegal access, deletion, corruption, mishandling and other malicious actions. Intrusion detection systems [8][16][24], cryptography [10], and web vulnerability assessment tools [6] are few of many other efforts to deal with emerging information security related issues. In short, technology is still the key element to solve any cyber security attacks.

3.1.3. Economy. Perhaps the most widely cited information security paper dealing with the economics perspective is one by Anderson [11] who discusses various perverse incentives in the information security domain. In [26] Gordon and Loeb present a framework to determine the optimal amount to invest to protect a given set of information. Later, Gordon, Loeb and Lucyshyn in [27] extend the study to show how secure information sharing can economically beneficial. Likewise, in [9] and [28] different economic analysis regarding information sharing and its relation to stock market are well argued.

3.1.4. Culture. Amongst other previous aspects, cultural aspect is the least aspect discussed in academic papers. On the other hand, it is widely proven that information security breaches are often caused by internal users of an organization [30]. Information security culture can be effectively achieved through integrating education and organizational leadership simultaneously [32][33]. Then it would become a natural behavior and responsibilities of any individuals within the organization [29]. Natural understanding about what is and what is not acceptable in respect to information security among users reflects the existence of information security culture [31].

3.2. Information Security Components

It is confirmed that confidentiality, integrity and availability (CIA) are three traditional components of information security widely accepted in information security literatures [10]. CIA is the essential objectives of information security management which is agreed by different type and level of organization [5][8]. Loosing one of them might threaten the organization to guarantee its level of security [14].

3.2.1. 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.

3.2.2. Integrity. It means that data cannot be modified without authorization. Integrity ensures that only authorized user able to access the data.

3.2.3. 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.

4. AHP Information Security Policy Model

Based on section 2, we define the model (see figure 1) based on AHP standard. Then we construct a survey to derive valuable inputs from prospective participants.

At the beginning stage, we focus on government officials in Indonesia. Later, we will extend the survey to other groups of participant (industry and university) in order to gain comprehensive thought from experts and professionals from different environments in this country.

4.1. AHP Process

Decision support system is one of operational research fields. Analytic Hierarchy Process (AHP) of Saaty [4] is a method that widely applied in many decision making fields [3][4]. It overcomes complexity of previous decision support methods. In addition, it gives a basis for eliciting, discussing, recording, and evaluating the elements of a decision. Moreover, it can be used to perform combination of both qualitative and quantitative into the same decision making methodology. AHP has been applied in many areas of research including few papers in computing and information technology [1][2].

In order to develop the AHP method, one should follow simple steps below [22]:

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).

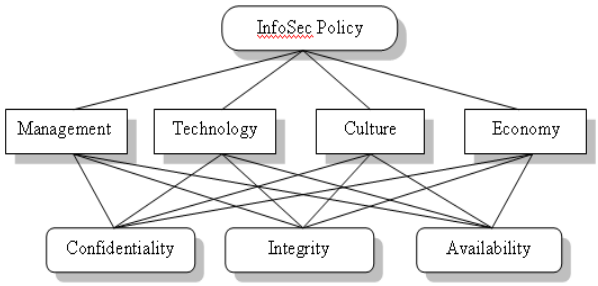

Figure 1. Information security policy model

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.
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.

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).

4.2. Analysis

Web-HIPRE is used to generate and analyze the model. It is a multi attribute decision support system which provides a set of analytical methods such as SMART, SMARTER, and AHP to support decision makers in the evaluation of different alternatives. It also supports AHP based group decision support for gaining the integrated result from many group

respondents [7]. The following figure shows the model generated with Web-HIPRE .

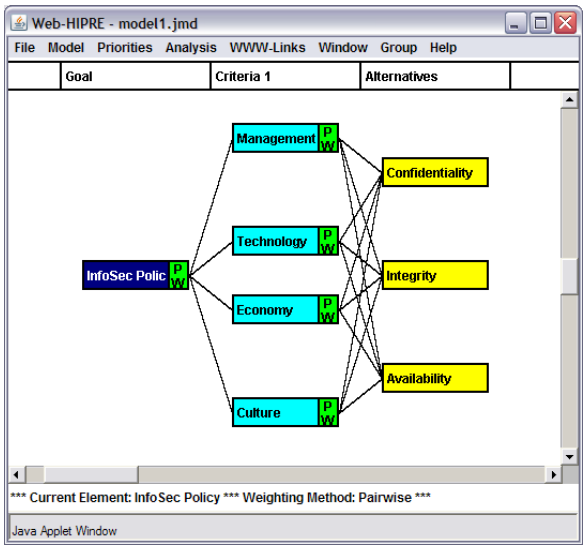

Figure 2. The model n Web-HIPRE

The hierarchy is based on figure 1, where there are four criteria (MTEC) and three alternatives (CIA) to achieve the goal.

5. Results and Discussion

Based on respondents' inputs, we could found complete paired comparison matrix as can be seen from the following table.

Table 1. Paired comparison matrix

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

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

Table 1.A expresses 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.

Then, Table 1.B to 1.E illustrate local weight of comparative alternatives according to criteria which describes specific local weight value of all three alternatives (confidentiality, integrity, and availability). In terms of consistency, it is important to explain that although both table 1.A and 1.B show a little inconsistency measures (0.127 and 0.121), it is still acceptable as long as it below 0.200 (as the maximum value for consistency measure or CM) [7]. Therefore, among all matrixes, the most appropriate result showed by table 1.E with CM value of 0.000 which means completely consistent.

Then, we perform the last step of AHP analysis by calculating all local weights and aggregate them into global weight value or composite overall priorities to obtain the overall priority.

The following figure shows the graph of composite overall priorities in Web-HIPRE.

Figure 3. Composite Overall Priorities

The result clearly indicates that technology and management are considered more important than economic and cultural considerations. This finding reflects imbalanced approach of information security policy development in government sector. Whereas, in order to be effectively applied, cultural insights [29] as well as economic perspectives [11] should be given more portions in shaping the information security policy development at government level.

This is inline with our previous findings in [12], that information security is one of e-government critical issues in Indonesia.

Then, the last step of the analysis processes is aggregating the total priority of both criteria and alternatives.

Table 2. 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***	

Table 2 shows the final rank or priority of to achieve information security policy as the goal. In terms of security alternatives, it is found that availability of 0.432 is preferred as the top requirement followed by confidentiality which accounted for 0.387. Integrity seems do not become priority within government agencies that only accounted for 0.181.

In addition, this final result also shows that there have been more concern on management and technology 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.

Based on these findings, it seems government agencies still with the focus on availability of data and information systems in its environment. This also reflects the top priority of information technology efforts by government agencies in Indonesia. However, to successfully achieve the goal, economic and cultural approaches are required to increase information security awareness of among government officials in different levels.

Therefore, we recommend three points, as follows:

- Economic aspects of information security should be clearly understood and addressed as one of important factors for Indonesian government in recent information era.
- Improve security awareness among government employees by adequate education and training to achieve sound security culture in government environment.
- 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.

5. Conclusion

This paper attempts to extend the general topic of information security policy into a specific environment, which is government information security policy. It describes the tenets of applying the Analytic Hierarchy Process to a simple model based on four criteria (MTEC) and three alternatives (CIA). Availability represents the highest priority followed by confidentiality and integrity. The study also shows the proportion of management and technology aspects significantly dominate the other two ones. Information security awareness through education is strongly recommended to deal with this disproportion.

In addition, this study justifies that the application of AHP method in information security is reasonable and it provides a robust and encompassing treatment for decision makers in both qualitative and quantitative ways. Therefore, it is reasonable to apply it in larger scope.

However, since it is indicated some correlation between criteria and alternatives in Figure-1 are in existence, additional study may be done with ANP (Analytic Network Process) method.

In the future, we also plan to extend the study with additional group participants from industry and university, and combining the results as group decision making for developing a model of information security policy with AHP or ANP methods.

6. References

[1] Ghotb, Fatemeh and Bruce, A. C, 1996, "Risk analysis of the end user computing", *Proceedings of the Fourth International Symposium on the Analytic Hierarchy Process*, Simon Frasier University, Burnaby, B. C. pp. 541-546.

[2] Vellore, R. C. and Olson, D. L., 1991, "An AHP application to computer system selection", *Mathematical and Computer Modeling*, vol. 15, no. 7, pp. 83-93.

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

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

[5] Leiwo, J., Gamage, C., and Zheng, Y. 1999, "Organizational modeling for efficient specification of information security requirements", *Advances in Databases and Information Systems: 3rd East European Conference*, ADBIS'99, Maribor, pp.247-60.

[6] Álvarez, G. and Petrovi, S., 2003, "A new taxonomy of Web attacks suitable for efficient encoding", *Computers & Security*, vol. 22, issue 5, pp. 435-449.

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

[8] Rosenthal, D., 2002, "Intrusion detection technology: leveraging the organization's security posture", *Information Systems Management*, vol. 19, no.1, pp.35-44.

[9] Schecter, S.E. and Michael,D.S., 2003, "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. pp. 122-137.

[10] Paterson, K.G., 2002, "Cryptography from Pairings: A Snapshot of Current Research", *Information Security Technical Report,* vol. 7, issue 3, pp. 41-54

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

[12] Hwang,J. and Syamsuddin,I. 2008, "Failure of E-Government Implementation: A Case Study of South Sulawesi", *Proceeding of IEEE International Conference on Convergence and Hybrid Information Technology ICCIT2008*, pp. 952-960.

[13] United Nation (2008), *UN E-Government Survey*, United Nations, New York

[14] Byrnes, F., Proctor, P., 2002, *Information security must balance business objectives*, [Online document],[cited 2009 January 09] Available HTTP http://informit.com

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

[16] Bauss, T., 2000, "Intrusion detection systems and multisensor data fusion", *Communications of the ACM,* vol. 43, issue 4 pp. 99 - 105

[17] Zviran, M., and Haga, W., 1999, "Password security: an empirical study", *Journal of Management Information Systems*, vol. 15 no.4, pp.161-85.

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

[19] Peltier, T., 2001, *Information Security Risk Analysis*, Auerbach Publications, CRC Press, USA.

[20] Chi,S.D., Park,J.S., Jung,K.C. and Lee,J.S., 2001, *Network Security Modeling and Cyber Attack Simulation Methodology, in Information Security and Privacy*, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 320-333

[21] Householder,A., Houle, K. and Dougherty, C, 2002, "Computer attack trends challenge Internet security", *Computer IEEE,* vol. 35, issue 4, pp. 5-7.

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

[23] Arbaugh, W.A., Shankar, N., Wan, Y.C.J. and Zhang,K., 2002 , "Your 80211 wireless network has no clothes", *IEEE Wireless Communications*, vol. 9, issue 6 pp. 44-51.

[24] Fuchsberger, A.,2005, "Intrusion Detection Systems and Intrusion Prevention Systems", *Information Security Technical Report*, vol. 10, issue 3, pp. 134-139

[25] Landwehr,C.E, 1981, "Formal Models for Computer Security", *ACM Computing Surveys*, vol. 13, issue 3, pp. 247-278

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

[27] Gordon, L. A., Loeb, M. P. and Lucyshyn, W., 2003, "Sharing Information on Computer Systems Security: An Economic Analysis", *Journal of Accounting and Public Policy*, vol 22, no. 6.

[28] Campbell, K., L. Gordon, L. A., Loeb, M. P., and Zhou, L.,2003, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market forthcoming", *Journal of Computer Security*. vol. 11, no. 3, 2003, pp. 431-448

[29] Schlienger, T., and Teufel,S., 2002, "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

[30] PriceWaterhouseCooper, *Global state of information security survey 2008*, [Online document],[cited 2008 December 27] Available HTTP http://www.pwc.com/extweb

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

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

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

[34] CSI, CSI 2008 Survey, [Online document],[cited 2008 December 27] Available HTTP http://www.gocsi.com