International Research Journal of Applied and Basic Sciences. Vol., 2 (11), 426-432, 2011
Available online at http://www. irjabs.com

IRJABS

STRATEGIC INFORMATION SECURITY DECISION MAKING WITH ANALYTIC HIERARCHY PROCESS

IRFAN SYAMSUDDIN

Department of Computer and Networking Engineering State Polytechnic of Ujung Pandang Makassar, Republic of Indonesia

***Corresponding author*:** E-mail: irfans@poliupg.ac.id

Abstract: Security is a serious concern in delivering trusted e-government services. However, in order to apply a sound security policy in e-government environment, strategic decision should be made while involving different point of views. 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.

***Key words*:** AHP, Information security; Policy; Decision making.

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 (2001). 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 sections, 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.

LITERATURE REVIEW

In this section, we briefly describe important aspects and components of information security policy. Dhillon and Blackhouse (2001) 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 that information security policy should become business priority as it has significant role to guarantee trust in digital age (Filipek, 2007). Information security related literatures show various matters attributed to information security policy. In this paper, they are classified into aspects of information security and components of information security. In general, aspects of information security can be ctegorized into management, technology, economy and culture. Information security management has been realized as essential in ensuring information handling within organization. Filipek (2007) states that it covers data classification, access control, etc.

On the other hand, technology of information security has been regarded as the most impoartent guard to ensure the security of information. Securing information technology in terms of data, hardware, and applications has been the most concerned aspect since the beginning computerized era. It includes computer security, wired and wireless network security and internet security (Householder, et.al, 2002).

Economy is another important aspect of information security. 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 (Anderson, 2001). 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 (2002). Through economic aspect, measurements of information security can be done quantitatively (Schecter and Michael, 2003).

Lastly is the aspect of security culture. Among the discussed aspects above, cultural perpective of information security 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 (Martins and Eloff, 2002). Therefore, internal security approaches are encouraged in the form of security awareness. It is affirmed by Thomson and von Solms (1998) that combination of security education with organizational leadership is the critical success factor for an organization to effectively promote security awareness and gradually develop a security culture within an organization.

Security component is regarded as security principles that should exist in order to ensure security of information has been archieved. Basically it consists of three main points, confidentiality, integrity and availability (known as CIA Triad). They are three traditional components of information security widely accepted in information security literatures (Filipek, 2007). It is often called security triad which should be fulfilled appropriately in order to achieve security objectives within an organization.

Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. It reflects protection of the privacy users in respect to their own information (Schecter and Michael, 2003).

Integrity means that data cannot be modified without authorization. Integrity should exist in order to ensure that only authorized user able to access the data (Filipek, 2007).

Availability is a property to guarantee 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 (Thomson and von Solms, 1998).

There is no doubt that confidentiality, integrity and availability are three components that should exist alltogether in order to guarantee that information is clearly confident in terms of protecting disclusure of information, without any kind of alteration or modification by unauthorized actions as well as it is available when required by authenticated person or systems.

PROPOSED DECISISON MODEL

With the aim to conduct evaluation on information security policy strategy, a new model as can be seen in figure 1 is proposed. 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.

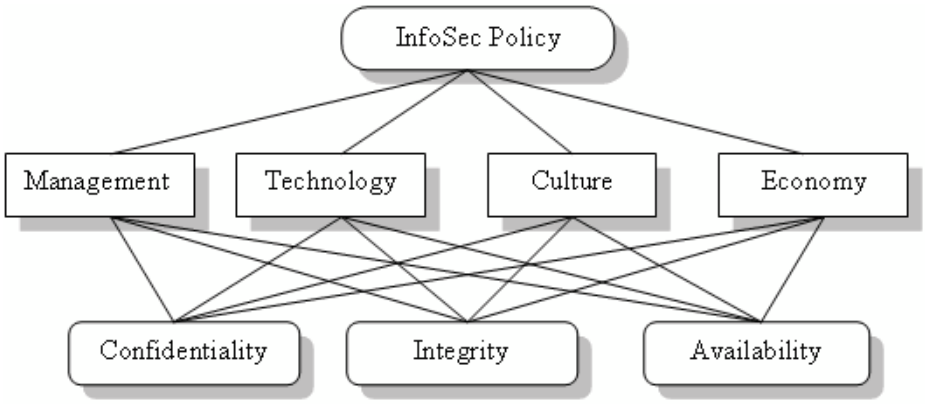

Figure 1. Proposed model of strategic information decision making.

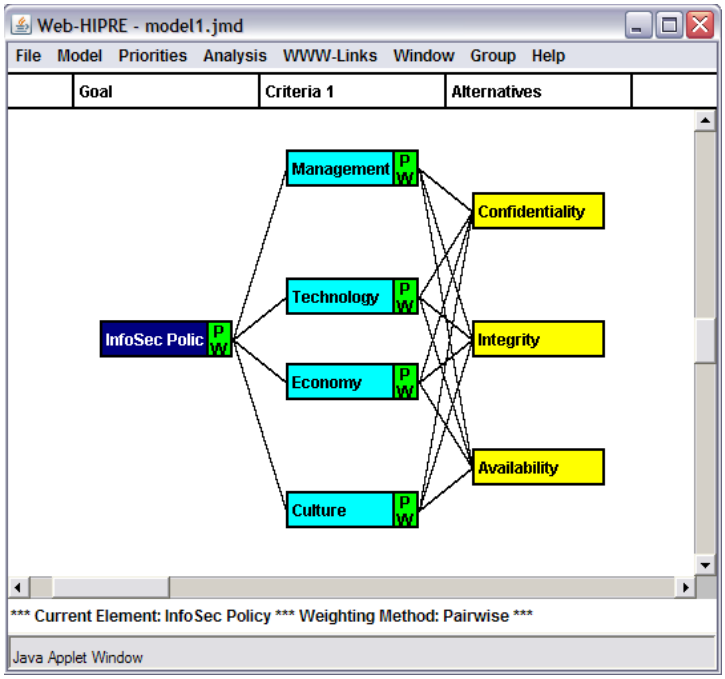

Figure 2. The AHP Evaluation model in Web-HIPRE.

A. Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) is a multi criteria decision analysis proposed by Saaty (1990). 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 decision making during the last twenty five years or more (Vadya and Kumar, 2006).

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 Saaty (1990):

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 from all layers (levels) are aggregated to obtain final weights of the decision alternatives (elements at the lowest level) The final weights represent final decision made by the decision makers.

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 (Mustajoki and Hämäläinen, 2000). Figure 2 shows our evaluation model developed in Web-HIPRE.

In Web-HIPRE the problem is structured hierarchically to form a value tree. In this value tree each criterium is divided to its subcriteria, which are weighted by their importance to decision maker (On the lowest level criteria the alternatives are weighted). The total weights of the alternatives are calculated from these local weights. Look also Creating a Model.The value tree in Web-HIPRE is build up by mouse-driven commands. To each element of the value tree can decision maker make a link to a Web-page located anywhere in the World Wide Web. This linked Web-page can contain any additional information about this element (sounds, images, etc.), which can help the decision maker to give weights more accurately (Mustajoki and Hämäläinen, 2000).

RESULT 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 (1990). It is often a 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.

Using WebHIPRE, all paired comparison matrix are performed 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

	M	T	E	C	LW
Management	1,00	1,00	4,00	5,00	0,40
Technology	1,00	1,00	3,00	7,00	0,42
Economy	0,25	0,33	1,00	1,00	0,10
Culture	0,20	0,14	1,00	1,00	0,08
			Consistency Ratio		0,127

TABLE II. PAIRWISE COMPARISON OF MANAGEMENT

	C	I	A	LW
Confidentiality	1,00	0,33	5,00	0,279
Integrity	3,00	1,00	7,00	0,649
Availability	0,20	0,14	1,00	0,072
		Consistency Ratio		0,121

TABLE III. PAIRWISE COMPARISON OF TECHNOLOGY

	C	I	A	LW
Confidentiality	1,00	0,33	5,00	0,279
Integrity	3,00	1,00	7,00	0,649
Availability	0,20	0,14	1,00	0,072
		Consistency Ratio		0,121

TABLE IV PAIRWISE COMPARISON OF ECONOMY

	C	I	A	LW
Confidentiality	1,00	0,33	5,00	0,279
Integrity	3,00	1,00	7,00	0,649
Availability	0,20	0,14	1,00	0,072
		Consistency Ratio		0,121

TABLE V. PAIRWISE COMPARISON OF CULTURE

	C	I	A	LW
Confidentiality	1,00	0,33	5,00	0,279
Integrity	3,00	1,00	7,00	0,649
Availability	0,20	0,14	1,00	0,072
		Consistency Ratio		0,121

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.

In addition, Table II. shows comparison matrix of alternatives CIA with respect to the Management criteria. Local weight of the three alternatives C, I, A are 0,279, 0,649 and 0,072 respectively with consistency ratio of 0,121.

Table III exhibits similar data with respect to Technology criteria. It is found that local weight of the three alternatives C, I, A are 0,062, 0,680 and 0,257 respectively with consistency ratio of 0,085.

Then, Table IV. shows comparison matrix of alternatives CIA with respect to the Economy criteria. In this table, it can be seen that local weight of the three alternatives C, I, A are 0,669, 0,243 and 0,088 respectively with consistency ratio of 0,042.

The last Table V represents comparison matrix of alternatives CIA with respect to the Culture criteria. It is calculated that local weight of the three alternatives C, I, A are 0,692, 0,231 and 0,077 respectively with consistency ratio of 0,000 means that the decision made by decision makers are 100% consistent.

After those steps, finally all local weights obtained in all layers (tables) are aggregated to obtain global weight value or composite overall priorities as a final weight of alternatives. The final result is represented in Table VI below.

TABLE VI FINAL RESULT

GOAL	C	I	A	GW
Management	0,029	0,112	0,261	0,402
Technology	0,282	0,026	0,107	0,415
Economy	0,700	0,025	0,009	0,104
Culture	0,006	0,018	0,055	0,079

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.

Another facts derived from this result is that there is an imbalanced approach in current information security strategy occurs in government.In order for information secuirty to be effectively applied, cultural insights as well as economic perspectives 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 (Syamsuddin and Hwang, 2008), which pointed out information security as one of the challenging issues to develop effective e-government systems in Indonesia.

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 in security aspect, management and technology aspects are found to be the highest concerns compare to economic and cultural aspects.

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.

Based on findings it is recommended to Improve security awareness among government employees by adequate education and training to achieve sound security culture in government environment.

Also, economic aspect of information security should be clearly understood and addressed as one of important factors for Indonesian government in recent information era.

In addition 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.

REFERENCES

Anderson R (2001) "Why Information Security is Hard : An Economic Perspective," Proc. of 17th Annual Computer Security Applications Conference, 2001, 10-14.

Dhillon G, Blackhouse J (2001) "Current directions in IS security research: towards socio-organizational perspectives", Information Systems Journal, 11(2), 127-53.

Filipek R (2007) "Information security becomes a business priority," Internal Auditor, 64(1),18-23.

Gordon LA, Loeb MP (2002) "The Economics of Investment in Information Security," ACM Transactions on Information and System Security, 5(4) 438-457.

Householder A, Houle K, Dougherty C (2002) "Computer attack trends challenge Internet security," Computer IEEE, 35(4), 5-7.

Martins A, Eloff J (2002) "Information security culture", IFIP TC11, 17th International Conference on Information Security, 203–214.

Mustajoki J, Hämäläinen RP (2000) "Web-HIPRE: Global decision support by value tree and AHP analysis," INFOR, 38(3). 208-220.

Saaty TL (1990) "The Analytic Hierarchy Process, RWS Publications", Pittsburgh, PA. 1990.

Schecter SE, Michael DS (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, 122-137.

Syamsuddin I, Hwang J (2008) "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, 2, 952-96

Thomson ME, von Solms R (1998) "Information security awareness: educating your users effectively," Information Management and Computer Security, 6(4), 167–173.

Vaidya OS, Kumar S (2006) "Analytic hierarchy process: An overview of applications", European Journal of Operational Research, 169(1), 1–29.

Zahedi F (1986) "The analytic hierarchy process—a survey of the method and its applications," Interfaces, 16(4) 96–108.