Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach

Jonathan Salar Cabrera[1,*], Ariel Roy Luceño Reyes[2], Cindy Almosura Lasco[1]

[1]Institute of Computing and Engineering, Davao Oriental State College of Science and Technology, Philippines

[2]College of Information and Computing, University of Southeastern Philippines, Philippines

Received 06 April 2020; received in revised form 08 August 2020; accepted 11 October 2020

DOI: https://doi.org/10.46604/aiti.2021.5476

Abstract

Security is the most serious concern in the digital environment. To provide a sound and firm security policy, a multi-holistic approach must be considered when making strategic decisions. Thus, the objective of this study was to evaluate the information security (IS) and decision making of Davao Oriental State University (DORSU) using the analytic hierarchy process (AHP) approach. The four aspects of IS, namely, the technology, management, economy, and culture were used with the three IS components consisting of confidentiality, integrity, and availability to implement the AHP. The results showed that the technology and management have higher significant values than the economic and cultural aspects. Meanwhile, for the IS components, the integrity signifies the highest priority followed by confidentiality, lastly, and availability. These results emphasize an imbalance in implementing IS policy, which must be addressed to ensure that the data integrity, confidentiality, and availability are balanced, particularly during the information exchange transactions.

Keywords: analytic hierarchy process, evaluation process, information security, prioritization

1. Introduction

Data is an essential element in the organization that needs to be protected. Therefore, attacks usually focus on the internal controls of the organization that enables the hampering of information. Such views on the importance of data-enabled modern organizations to take an advanced step in ensuring that data is protected from unauthorized access. This involves integrating technology and the employment of governance and policy enforcement mechanisms to guarantee data protection and compliance. First-world countries like the USA and the United Kingdom have been strengthening their laws and regulations on information security (IS) to prevent unwanted events such as the recent Facebook–Cambridge Analytica data scandal. It is unfortunate that, in the Philippines, the current setting of its IS law does not conform yet to the current trend of the IS environment. However, in terms of IS control and security, organizations can follow international standards.

Deciding to make the best decision of what security policies to implement is a challenging task, especially when there are several aspects to consider. In the fast-changing information age, the IS policy in the organization is also evolving to catch-up with the change. Subsequently, all possible options in the IS aspects should be considered to develop effective and appropriate policy. Literature shows that IS developments mainly focused on technical and managerial aspects [1]. However, in the information age, information technology is merely affecting cultural and economic aspects. Combining cultural, economic, technology, and management aspects into IS-related decisions expand the views from different perspectives. Hence, a suitable and appropriate method is highly required to analyze by incorporating those aspects carefully. Thus, MCDA is highly recommended.

[*] Corresponding author. E-mail address: jonathan.cabrera@doscst.edu.ph

In this paper, the AHP approach under MCDA is used to evaluate the IS decision making of Davao Oriental State University (DORSU). Section 2 describes the related literature of the components and aspects of the information security applied in this study. Section 3 discussed the methodology with the MCDA-AHP evaluation together with partial results as the steps progress. The results and discussions are discussed in section 4, whereas the conclusion and the recommendations are given in section 5.

2. Literature Review

It is necessary to briefly review the elements of the information system to fully understand the importance of information security. Typically, information systems in an organizational setting are blends of software, hardware, and telecommunications networks to collect, produce, and distribute a useful data [2]. On the other hand, IS is defined as creating a set of practices that keeps the information and information systems secure from the unauthorized access, usage, leakage, retardation, alteration, or destruction [3-4]. With the significance of the information security, its role is vital due to the digitalization of the business processes of the organization. Sharing information using various information technologies provides risk. As a result, security is highly needed. In the fast-changing information era, IS plays an important role that the organization should put IS as a priority to secure thrust in the digital environment. Further, works about information show various matters concerning IS policy [5-7].

The Confidentiality, Integrity, and Availability (CIA) triad is considered as the core principle of IS [8]. However, as stated in the Five Pillar Information Assurance data security model [9-10], a continuous debate suggests that aside from confidentiality, integrity, and availability, the IS core principle can still be extended to include authenticity and non-repudiation features. CIA, or often called the security triad, should always fulfill to achieve the IS objectives in the organization. Confidentiality, as the first component of the CIA triad, denotes thwarting the information leakage to adversaries which is very essential in maintaining the secrecy of personal information held by the system [8]. Integrity, on the other hand, is the second component of the CIA triad and lies in upholding and assuring the truthfulness and dependability of data. This component denotes that modifications on data must not be made without authorization or proper consent to conduct data changes. Aside from the confidentiality, it is necessary that IS must provide a message integrity, which refers to ensuring that messages have never been modified, altered or tampered with [8]. Lastly, the availability, the third out of three components of the CIA triad, is thought as a must since it is significant for any information system to be accessible whenever it is needed. It means that the proper functionality of the computing systems which are to store, process, access, and protect the information must be maintained to ensure the accessibility of security controls and communication channels at all times. Guaranteeing availability also encompasses prevention from denial-of-service attacks [8].

Subsequently, the CIA is always a part of the IS aspects, referring to the perspectives of the organization or business. Mostly, the organization focuses on the management and technical aspects of IS [1]. Furthermore, recent studies are giving high emphasis on cultural [11] and economic aspects [12] in the information security. In general, aspects of the information security can be categorized into the technology, management, culture, and economy. Technology is the most vital guard to ensure the security of information [13]. Since the start of the digital age, apprehensions were mostly directed to safeguarding information, and technology, which includes hardware, information/data, and applications. Computers, wired/wireless networks, and internet security were amongst the primary concern [14]. Likewise, the management in information security is all about ensuring information handling in the organization. While the economy is another crucial aspect of IS, it has been recently recognized that economic concerns play a noteworthy role in warranting the level of security measures within an organization [1]. By disregarding the different economic aspects involved in IS which includes investment, incentives, and financial information sharing, it will be difficult to determine the economic benefit of such protections [15]. Accordingly, a measurement of the economic aspect of IS can be done quantitatively. Last of all, the cultural aspect of information security refers to human attributes such as behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization [16]. It is also the least important aspect in almost all organizations. In addition, as stated by Ngo et al. [17], information security culture is formed by the conventional conduct and actions of workforces and the organization as a whole, and how things are done.

In overall assessment in the information security aspect, the three components (i.e., confidentiality, integrity, and availability) should exist altogether to guarantee that the information is confident in terms of protecting disclosure of information, without any alteration or modification by unauthorized actions as well as it is available when required by authenticated person or systems [13].

3. Methodology

Information security policies are critical because they must be able to review the risk appetite of an organization's management. The proper evaluation of IS policies will not only address the need of an organization to create a mechanism that protects it from internal and external threats, but also help in directing a managerial mindset on implementing security within the organization [18]. Hence, with such high regard on the safety, the methodology of this paper is focused mainly on evaluating IS policy using the AHP framework under MCDA concepts as shown in Fig. 1. This approach has three levels: goal, criteria, and indicators. The goal is top-level, which specifies the objective of this paper: the information security policy evaluation; the second level is the criteria, which are four aspects of the information security policy; and last but not least, the indicators which are the three security components.

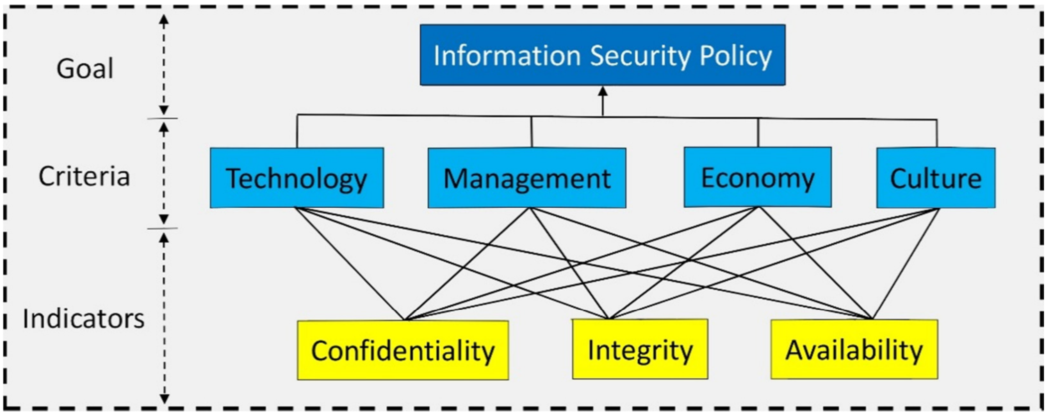

Fig. 1 MCDA-AHP framework for information security policy assessment

MCDA is a useful and valuable tool when applying complex decisions. Using a structured approach, MCDA analyzes and measures a series of alternatives or criteria to discern their relative importance and identify which criterion is the most significant. Likewise, the AHP is an MCDA approach and a decision support tool introduced by Saaty [19-20]. AHP is a hierarchical approach tool used to solve complex decision problems. The AHP hierarchy is a top to bottom approach, from the top is the goal, criteria are in the middle, and at the bottom is the indicators presented in Fig. 1 [21]. The weights of each criterion and indicators must be determined using pairwise comparisons. The weights of the criteria and indicators show the importance of decision making.

There are six steps to process a complex problem using AHP [19, 22]. As described in the paper of Cabrera & Lee [21], the first step is when the problem has already been identified, break the problem down into its component factors. Second, these component factors are arranged and constructed into a hierarchy, then a pairwise comparison matrix is built on the third step. Hence, the decision-makers (DM) can systematically assess the alternatives for each of the chosen criteria or indicators. During the fourth step, the weights of each criterion are calculated based on the values assigned by the DM and on the fifth step, the results are then analyzed to establish the prioritization of the criteria and indicators. After that, the consistency is checked to determine the reliability of the results.

The consistency ratio (CR) is the key component of AHP. The CR should be less than 10%, so that the comparison matrix is considered acceptable, and the judgements of the DM are reliable (see sub-section 3.3 for the computation). The succeeding sub-sections are the processes to come up with the acceptable relative weights in every criterion and indicators.

3.1. Pairwise comparison

In order to use the AHP, a pairwise comparison matrix must be conducted first. This was done by comparing each criterion of the study based on Saaty's scale [19] as displayed in Table 1. The results were in integer values (i.e., 1 to 9). The higher number means that the chosen factor is more important than the other.

Table 1 The fundamental scale and its description as described by Cabrera & Lee [21]

Scale	Judgement of Preference	Description
1	Equally important	Two factors contribute equally to the objective
3	Moderate	Experience and judgement slightly favor one over the other
5	Strong	Experience and judgement strongly favor one over the other
7	Very strong	Experience and judgement very strongly favor one over the other
9	Extremely important	The evidence favoring one over other is of the highest possible validity
2, 4, 6, 8	Intermediate values	When compromise is needed

3.2. Normalization

The normalization in AHP is a probability assigned to the suitability of each alternative. This step used the normalized matrix. This matrix is used to add the values in each column. In the pairwise comparison matrix, the entry in each column is divided by the sum of the column. Then, the result will be input in the corresponding cell in the normalized matrix. If the total value in the column is 1, the results in all cells in the column are normalized values as described in Eq. (1). Finally, the priority vector (PV) (i.e., the weights of the criterion or indicator) is computed by dividing the sum of the column of the matrix by the number of criteria used (n), as shown in Eq. (2), The C_{ij} in Eq. (1) refers to the value of a criterion or indicator in the pairwise comparison matrix. The X_{ij} is the normalized score, while PV_{ij} refers to the weights of each criterion or indicator. The PVs give the relative importance weights of the criteria or indicators.

$$X_{ij} = C_{ij} / \sum_{i=1}^{n} C_{ij} \tag{1}$$

$$PV_{ij} = \sum_{j=1}^{n} X_{ij} / n \tag{2}$$

3.3. Consistency analysis

The consistency analysis (CA) is the last process in AHP. In order to derive the CR, the CA process has to undergo three steps. The first step is to calculate the consistency measure (CM) which can be obtained through multiplying the pairwise matrix with the PV. The result is then divided into the weighted sum vector with its criterion weights. The second step is calculating the consistency index (CI) as described in Eq. (3). The λ_{max} refers to the sum of the CM divided by the n (i.e., number of criteria or indicators). Finally, the CR is computed by the CI over the RI as described in Eq. (4).

$$CI = (\lambda_{\max} - n) / (n-1) \tag{3}$$

$$CR = CI / RI \tag{4}$$

The λ_{max} values are set to 4.03, 3.01, 3.01, 3.04, and 3.07 for the goal, technology, management, economy, and culture, respectively. The values of the random index (RI) developed by Saaty [20]and its corresponding number of compared criteria are 0.00, 0.58, 0.90, 1.12, 1.24, 1.32, and 1.41 for the 2, 3, 4, 5, 6, 7, and 8, respectively.

4. Results and Discussion

The advantage of AHP is the ability to quantify the inconsistency in the judgment of the decision-makers. As stated by Saaty [19, 22], the CR should be less than ten percent (10%) to guarantee that the decision is reasonably correct. If inconsistency occurs, the survey should be repeated until the CR is less than ten percent (10%). The survey should be repeated in cases where CR is less than ten percent to guarantee the level of consistency at an acceptable level.

The researchers fulfilled the pairwise comparison matrix from the survey conducted to the IT head of the Davao Oriental State University. The IT Head is responsible for managing and supervising the IT functions of the University, which includes one main campus and three external campuses, situated on different municipalities in the province of Davao Oriental. As of this writing, the University has an overall population of approximately 10,000 students with all these data stored in the electronic school's management system (ESMS) and access to the school's e-learning management system (ELMS) that are both administered and managed by the Information Technology Services Unit.

There were five comparison matrices created, representing the IT head's opinion in the current IS policy implementations according to the AHP framework. In terms of the IS policy, the technology criterion is highly prioritized, followed by management, economy, and cultural aspect, respectively as shown in Table 2.

Table 2 Matrix concerning the goal

Criteria	T	M	E	C
Technology (T)	1	2	3	4
Management (M)	0.5	1	2	3
Economy (E)	0.33	0.5	1	2
Culture (C)	0.25	0.33	0.5	1
SUM	2.08	3.83	6.5	10

Moreover, Tables 3-6 show the importance of the three alternatives (i.e., confidentiality, integrity, and availability) for every single criterion. In the technology perspective, integrity is highly prioritized followed by availability and confidentiality. In the case of management, the topmost priority is the integrity. The next is the confidentiality and the last is the availability. Finally, economically and culturally speaking, the confidentiality indicator is prioritized followed by the integrity and availability.

Table 3 Pairwise comparison matrix concerning technology

Criteria	C	I	A
Confidentiality (C)	1.00	0.33	0.50
Integrity (I)	3.00	1.00	2.00
Availability (A)	2.00	0.50	1.00
SUM	6.00	1.83	3.50

Table 4 Pairwise comparison matrix concerning the management

Criteria	C	I	A
Confidentiality (C)	1.00	0.50	2.00
Integrity (I)	2.00	1.00	3.00
Availability (A)	0.50	0.33	1.00
SUM	3.50	1.83	6.00

Table 5 Pairwise comparison matrix concerning the economy

Criteria	C	I	A
Confidentiality (C)	1.00	3.00	5.00
Integrity (I)	0.33	1.00	3.00
Availability (A)	0.20	0.33	1.00
SUM	1.53	4.33	9.00

Table 6 Pairwise comparison concerning the culture

Criteria	C	I	A
Confidentiality (C)	1.00	3.00	4.00
Integrity (I)	0.33	1.00	3.00
Availability (A)	0.25	0.33	1.00
SUM	1.58	4.33	8.00

On the other hand, Tables 7-11 show the normalized matrix derived from Tables 2-6, respectively, which are the pairwise comparison matrices. Table 7 shows the percentage value of the criteria concerning the goal. It is revealed that technology is the dominant aspect of the overall IS policy perspectives, which accounted for 47% followed by 28%, 16%, and 10% for the management, economy, and culture.

Furthermore, Tables 8-11 represent the PV (i.e., weight) of the three alternatives (i.e., confidentiality, integrity, and availability). Table 8 shows that integrity is rank first with a 54% allocation in choosing the technology aspect in IS. The availability and confidentiality are only 30% and 16%, respectively. Also, the management aspect, integrity is prioritized first with 54% followed by confidentiality with 30% and 16% for availability (see Table 9). From the economic point of view, the confidentiality is significantly vital with an accounted value of 63%, while the integrity and availability are 26% and 11%, respectively as shown in Table 10. Looking at the cultural perspective, as shown in Table 11, confidentiality is highly emphasized with a value of 61%. The next is 27% for integrity and 12% for availability.

Table 7 Normalized matrix with the relative weights concerning the goal

Criteria	T	M	E	C	Total	PV	CM
T	0.48	0.52	0.46	0.40	1.86	0.47	4.05
M	0.24	0.26	0.31	0.30	1.11	0.28	4.04
E	0.16	0.13	0.15	0.20	0.64	0.16	4.02
C	0.12	0.09	0.08	0.10	0.38	0.10	4.02
SUM	1.00	1.00	1.00	1.00	-	1.00	-

Table 8 Normalized matrix with the relative weights concerning the technology

Indicators	C	I	A	Total	PV	CM
C	0.17	0.18	0.14	0.49	0.16	3.00
I	0.50	0.55	0.57	1.62	0.54	3.01
A	0.33	0.27	0.29	0.89	0.30	3.01
SUM	1.00	1.00	1.00	-	1.00	-

Table 9 Normalized matrix with the relative weights concerning the management

Indicators	C	I	A	Total	PV	CM
C	0.29	0.27	0.33	0.89	0.30	3.01
I	0.57	0.55	0.50	1.62	0.54	3.01
A	0.14	0.18	0.17	0.49	0.16	3.00
SUM	1.00	1.00	1.00	-	1.00	-

Table 10 Normalized matrix with the relative weights concerning the economy

Indicators	C	I	A	Total	PV	CM
C	0.65	0.69	0.56	1.90	0.63	3.07
I	0.22	0.23	0.33	0.78	0.26	3.03
A	0.13	0.08	0.11	0.32	0.11	3.01
SUM	1.00	1.00	1.00	-	1.00	-

Table 11 Normalized matrix with the relative weights concerning the culture

Indicators	C	I	A	Total	PV	CM
C	0.63	0.69	0.50	1.82	0.61	3.13
I	0.21	0.23	0.38	0.82	0.27	3.07
A	0.16	0.08	0.13	0.36	0.12	3.02
SUM	1.00	1.00	1.00	-	1.00	-

To determine the correctness of the percentage value stipulated in the previous paragraph, CR has to be computed. The CR was found to be 1.1%, 0.8%, 0.8%, 3.3%, and 6.4% for the goal, technology, management, economy, and culture, individually. The CR results specify that in the pairwise comparison and it showed that there is an adequate level of coherency. Thus, it can be concluded that the values are coherently acceptable.

The last goal of the analysis is to generate global or overall priorities as the final weight of the indicators. The result is shown in Table 12 and Fig. 2 and 3. Based on the results, it can be concluded that integrity is observed as the main priority as compared to confidentiality and availability. Integrity accounted for 47%, while confidentiality and availability were 32% and 22%, respectively as shown in Fig. 3.

Table 12 The overall weight of the indicators

Goal	Confidentiality	Integrity	Availability	Overall
Technology	0.075	0.254	0.141	0.470
Management	0.084	0.151	0.045	0.280
Economy	0.101	0.042	0.018	0.161
Culture	0.061	0.027	0.012	0.100
Overall	0.321	0.473	0.216	-

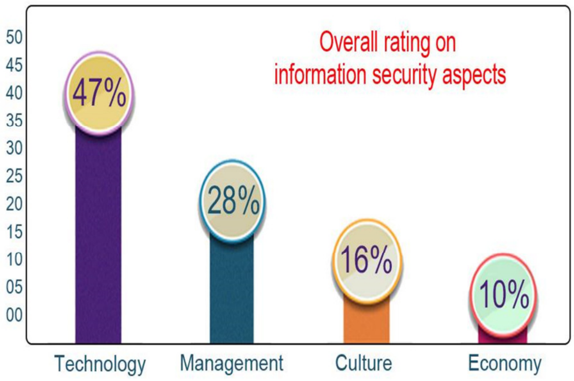

Fig. 2 Overall rating on information security aspects

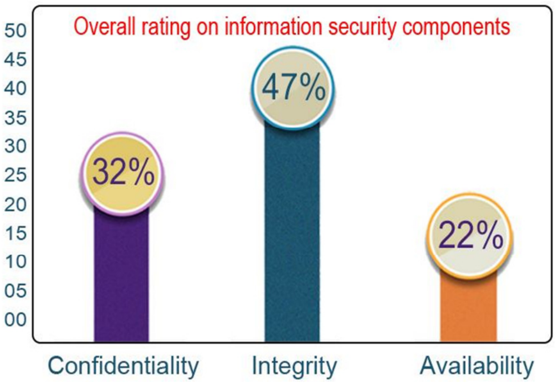

Fig. 3 Overall rating on information security components

In the information security aspects, the evaluation result showed that technology is the most important followed by the management while the economic and cultural aspects of IS gained the third and fourth spots, correspondingly. As evident to its overall ratings, particularly, DORSU has placed more serious concern on technology with 47% of the ratings, as compared to management with 28%, the economy with 16%, and 10% for culture (see Fig. 2).

The result reflects that the DORSU implementation for information security policy is imbalanced. Various literature shows the importance of cultural [11, 23-25] and economic aspect [12, 16] as the basis on the effective and balances information security policy implementations. The result also shows that information security is a challenging issue in DORSU governance.

5. Conclusions and Recommendations

This study gives a good reason for the application of the AHP approach in the evaluation of IS policy. Integrating multiple criteria and indicators in the MCDA shows a tangible advantage. The MCDA-AHP approach showcases the ability to check the inconsistency judgement of the decision-makers in a various criteria scenario. What is more, this approach also displays that decision-makers will be assisted in evaluating the implementation of the IS policy. In the aspect of IS, technology is found to be the highest priority. Likewise, concerning the IS component, integrity signifies the highest priority followed by confidentiality and availability.

Based on the results of this paper, the following recommendations are identified. First, improve the employee’s security awareness by providing training to achieve a comprehensive IS culture in the organization. Second, economic aspects should be addressed as part of the important factors in IS policy. Finally, it is essential to note that data integrity, confidentiality, and availability should be balanced, particularly during information exchange transactions bound outside in the organization’s computer networks [26].

Other MCDA approaches like Analytic Network Process (ANP) and fuzzy AHP/ANP can also be explored in the future to validate the result in other perspectives. Besides, expanding the number of respondents that will include all known decision-makers in the organization that may or may not have an IT background in order to give a generalized and holistic view of the result.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] R. Anderson, "Why Information Security is Hard: An Economic Perspective," Proc. Annual Computer Security Applications Conference, December 2001, pp. 358-365.

[2] J. P. Laudon and K. C. Laudon, Management Information Systems: Managing the Digital Firm, 12th ed. England: Pearson Education Limited, 2012.

[3] S. Shackleford, A. Proia, B. Martell, and A. Craig, "Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity," Texas International Law Journal, no. 291, 2015.

[4] Y. P. Surwade and H. J. Patil, "Information Security," E-Journal of Library and Information Science, pp. 458-466, January 2019.

[5] A. Singh, A. Vaish, and P. K. Keserwani, "Information Security: Components and Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 1, pp. 1072-1077, January 2014.

[6] A. R. Otero, Information Technology Control and Audit, 5th ed. New York: Auerbach Publications, 2018.

[7] S. Mishra and G. Dhillon, "Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment," Proc. European Conference on Information Systems (ECIS 2008), January 2008.

[8] D. La Marca, "Aspects of IT Security," https://www.mediabuzz.com.sg/research-aug-13/aspects-of-it-security, December 02, 2019.

[9] K. Brauer, "Authentication and Security Aspects in an International Multi-User Network," Turku University of Applied Sciences, Thesis, May 17, 2011.

[10] H. Moghaddasi, S. Sajjadi, and M. Kamkarhaghighi, "Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model," The Open Medical Informatics Journal, vol. 10, pp.4-10, October, 2016.

[11] A. Alhogail and A. Mirza, "Information Security Culture: A Definition and a Literature Review," World Congress on Computer Applications and Information Systems, IEEE Press, October 2014.

[12] L. Xu, Y. Li, and J. Fu, "Cybersecurity Investment Allocation for a Multi-Branch Firm: Modeling and Optimization," Mathematics, vol. 7, no. 7, pp. 1-20, July 2019.

[13] I. Syamsuddin, "Strategic Information Security Decision Making with Analytic Hierarchy Process," International Research Journal of Applied Basic Sciences, vol. 2, no. 11, pp. 426-432, 2011.

[14] I. Syamsuddin and J. Hwang, "The Application of AHP to Evaluate Information Security Policy Decision," International Journal of Simulation: Systems, Science and Technology, vol. 10, pp. 46-50, 2014.

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

[16] G. Dhillon, Principles of Information Systems Security: Texts and Cases, 1st ed., John Wiley & Sons, 2007.

[17] L. Ngo, W. Zhou, and M. Warren, "Understanding Transition towards Information Security Culture Change," Australian Information Security Management Conference, June 2014, pp. 67-73.

[18] R. Dunham, "Information Security Policies: Why They Are Important to Your Organization," https://linfordco.com/blog/information-security-policies/, May 5, 2020.

[19] T. L. Saaty, The Analytic Hierarchy Process: Planning, Priority Setting Resource Allocation, New York: Mc Graw-Hill, 1980.

[20] T. L. Saaty, "A Scaling Method for Priorities in Hierarchical Structures," Journal of Mathematical Psychology, vol. 15, no. 3, pp. 234-281, June 1977.

[21] J. S. Cabrera and H. S. Lee, "Impacts of Climate Change on Flood-Prone Areas in Davao Oriental, Philippines," Water vol. 10, no. 7, 893, July 2018.

[22] T. L. Saaty, Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World, 3rd ed. Pittsburgh: RWS Publications, 2012.

[23] Z. Milanović, "Information-Security Culture of Youth in Serbia," FBIM Transactions, vol. 7, no. 1, pp. 110-118, April 2019.

[24] T. Schlienger and S. Teufel, "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture," International Workshop on Database and Expert Systems Applications, September 2003, pp. 405-409.

[25] L. V. Astakhova, "The Concept of the Information-Security Culture," Scientific and Technical Information Processing, vol. 41, no. 1, pp. 22-28, April 2014.

[26] J. Hwang and I. Syamsuddin, "Information Security Policy Decision Making: An Analytical Hierarchy Process Approach," Third Asia International Conference on Modeling & Simulation, May 2009, pp. 158-163.