Analysis of College Students' Cybersecurity Awareness In Indonesia

Balqis Rofiqoh Chasanah, Candiwan
Telkom University
Dayeuhkolot, Bandung, Indonesia
balqisrc@gmail.com, candiwan@telkomuniversity.ac.id

Abstract— Internet-based attacks have become common and are expected to happen continuously with the development of technology. Therefore, cybersecurity emerged as an important concept in everyday life. It is defined as the protection of cyberspace. Cybersecurity Awareness (CSA) exists as a major defense key in protecting users and systems from internet-based attacks. The research presented in this study aims to assess the level of CSA among college students in Indonesia. This study uses the Analytic Hierarchy Process (AHP) method to test students in three dimensions, including attitudes, knowledge, and behavior. To measure this dimension, six focus areas in the topic of cybersecurity were taken and developed from previous studies on the same topic. The six focus areas are password security, cyberbullying, phishing, malware, identity theft, and the last is downloading, sharing and use of pirated content. The results showed that the total level of CSA for college students in Indonesia was in the good criteria. This is indicated by a total percentage of awareness around 80%. Nevertheless there are some focus areas that can be improved to increase the percentage.

Keywords— Analytical Hierarchy Process (AHP), Awareness, Cybersecurity, Cyber Threat, Cyber Attack

I. INTRODUCTION

More than 4.5 billion people are using the internet in early 2020, and there were approximately 175.4 million Indonesian internet users in January 2020 [1]. Almost 64% of Indonesia's total population is connected and already using the internet network in January 2020, and 59% of them are active users of social media, equivalent to 160 million active users [1]. Indonesia is one of the countries with a young population among other countries in the world. Based on the rankings in 2019, the median age of Indonesian population is 29.7 years old [2]. This number is below the global average of 30.9 years. However, Indonesian median age with a young population is considered opportunities for Indonesia to be more developed in the world of digital technology. Something similar happened in 2018. The total median age of the Indonesian population is 29.3 years. Users aged 15 to 29 years reached a high percentage of more than 80%. While the age range of 15-19 years is 91%, the age range of 20-24 years is 88.5%, then the age range of 25-29 years is as much as 82.7% [3].

The rapid development in information and communication technology sector not only has a positive impact on people's lifestyles, but also poses a threat to cyber security in Indonesia. The threat is called cyber-attack, which is an illegal or unwanted activity that aims to interfere, change, attack, or steal important data [4]. Cyber-attack has the potential to disintegrate the country's economy and disrupt state security [4]. It was identified that Indonesian internet users are quite vulnerable to cyber attacks. Also, Indonesian internet penetration data shows a growing number of users, which leads to an increase in people's dependence on technology, and the possibility of cyber crime. Indonesia is said to be the 34th country out of more than 150 countries in the world that is vulnerable to cyber threats and attacks [5]. This might happen because Indonesian internet users' cybersecurity awareness are lacking.

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

Lack of cybersecurity awareness brings some cases for some Indonesian internet users and the country. For example, it is said that Indonesia's losses due to piracy are predicted to reach tens of trillions of rupiah per year [6]. Indonesian Deputy Facilitator of Intellectual Property Rights and Regulation of the Creative Economy Agency, Ari Juliano Gema, said there is no comprehensive data on potential losses. But based on data collected from a number of institutions, the value of losses is huge. The potential loss is due to the distribution of pirated DVDs and illegal downloading of digital content [6]. In terms of password security, there were approximately 530,000 password and account data from the Zoom application, video conferencing software, have been trafficked by hackers on the Dark Web. To avoid data theft, some of Indonesian cyber security experts call on users to use a different password for each application and other website [7]. There is another case in Yogyakarta, where a 22 years old student named BS drained his own friend's money that is worth hunders of millions by falsifying his data [8]. In Indonesia, malware is also indicated as one of the most common cyber attacks. Nearly half of cyber attacks are caused by malware. Director of the National Cyber and Code Agency (BSSN) Threat Detection Agency, Sulistyo, said that there is a need to build awareness and train students in cybersecurity. Including cooperation with the police [9].

As a result of threats or negative influences from the internet, cybersecurity emerged as an important concept in the security of information technology. Cybersecurity awareness (CSA) is the main form of defense in information and system protection [10]. There are several important actors involved in cybersecurity system in Indonesia. These actors are divided based on their approach to cybersecurity: (1) Government; (2) Private sector; (3) Civil society; (4) Academics; and (5) Technical community. Within each category, there are some institutions that are considered directly responsible for cybersecurity, although there is also the possibility of one institution to discuss more than one particular problem or approach. The division of this category is based on observations towards the work of each actor [10]. Many security infringement have occurred at universities in Indonesia in various forms, such as penetration of the official website, website deface, and penetration to academic system to change the scores [11]. Based on this aspect, the authors are interested in conducting research on one of cybersecurity actors, specifically Indonesian college students. This research was conducted to determine cybersecurity awareness level of college students so that readers would understand the negative impacts they could get by neglecting the cybersecurity-related policies.

II. METHOD

Analytical Hierarchy Process is a decision support model developed by Thomas L. Saaty which is used to decompose complex multi-factor or multi-criteria problems into a hierarchy [12]. In the AHP method, the problem of decision making is decomposed into a hierarchy. At the top of the hierarchy is the goal of decision making. Criteria are at the next level and can be decomposed into sub-criteria. At the last level are the alternatives. By using pairwise comparisons and judgements from decision makers, priorities of alternatives and criteria weights are calculated. The importance of the Analytical Hierarchy Process method is explained in Table 1.

Table 1. Level of Importance in AHP

Intensity of Importance	Definition
1	Equal importance
3	Somewhat more important
5	Much more important
7	Very much more important
9	Absolutely more important
2, 4, 6, 8	Intermediate values

This type of research is quantitative where the data is collected by a questionnaire. The questionnaire used a nominal scale type and

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

dichotomous scaling method. Validity test is used to determine the feasibility of the items in the questionnaire and defining a variable [13]. The population in this research is not exactly known. Therefore to determine the sample in this research, Bernoulli formula is used with the calculation as below.

$$n = \frac{z^2 c.l\ pq}{E^2} \quad \text{.....(1)}$$

n = Number of Samples
$z^2c.l$ = The square of success rate
p = Proportion of success estimates
q = 1 – p, or the estimated proportion of failure
E = Error rate that is still acceptable

This research used a confidence level of 95% so that the value of Z = 1.96 is obtained. The error rate is set at 5%. By substituting these values to the equations that have been provided, the result is:

$$n = \frac{(1.96)^2(0.5)(0.5)}{(0.05)^2}$$

$$n = 384.16$$

From the results of the calculation above, Bernoulli's formula required at least 384 samples. Therefore, to facilitate the further calculation process, the number of respondents to be taken in this study is 400 people. This research has 54 questions about cybersecurity awareness to test Indonesian college students' attitude, knowledge, and behavior. Some questions are answered on a 3-point scale consisting of "yes", "do not know", and "no", while others only require answers on a 2-point scale consisting of "yes" or "no". These are some examples of questions from each dimension that can be seen in Table 2.

Table 2. Sample Questions

Dimension	Statement	Answer
Knowledge	If I don't maintain the security of my password, I could experience security problems in cyberspace (A1.1)	1. Yes 2. Don't Know 3. No
Attitude	I realized that if I didn't maintain the security of my password, I could experience security problems in cyberspace (B1.1)	1. Yes 2. Don't Know 3. No
Behavior	I always keep my password secure to avoid security breaches in cyberspace (C1.1)	1. Yes 2. No

The dimensional research framework is adapted from Sari et al. [14], and the focus areas were adapted from Chandarman et al [15]. The focus area used are approaches related to cybersecurity. The following figure is the research framework adopted from Sari et al. [14] and Chandarman et al. [15] shown in Figure 1.

(1)

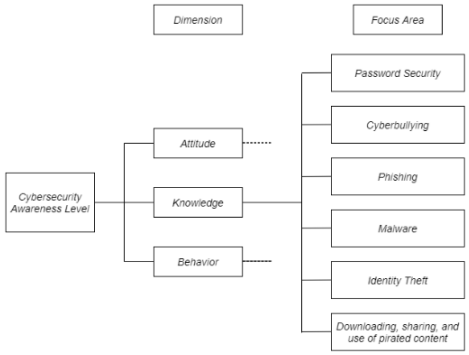

Figure 1. Research Framework

There are a total of 6 focus areas used, (a) password security, (b) cyberbullying, (c) phishing, (d) malware, (e) identity theft, (f) downloading, sharing, and use of pirated content [15]. From the framework and the specified focus areas above, several question indicators were made for this research.

AHP approach is also used to weight each focus area and dimension according to the level of importance. It used pairwise comparison to evaluate subjective factors, and these are based on professional judgment and opinions [16]. Comparisons are made using a preference scale, which gives numerical values to various preference levels [16].

Table 3. Dimension Weighting Value

Dimension	Weighting Value
Knowlegde	30%
Attitude	20%
Behavior	50%

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

The dimensions of behavior need more attention and are followed by the dimensions of knowledge and attitude [16]. Weighting is carried out before calculation based on predetermined weights. Weighting is done on each dimension (attitude, knowledge, and behavior), and focus areas (password security (a), cyberbullying (b), phishing (c), malware (d), identity theft (e), downloading, sharing, and use of pirated content (f)). The weighting value of the focus areas is done by assuming that each focus area has the same level of importance or equally important.

After deciding the level of importance for each focus area, then the level of importance will be normalized and calculated to get a weighting value (%) for each focus area. This normalization is done by formulas and manual calculations through Microsoft Excel. After normalizing each focus area, the next step is to find the average for each focus area. Focus area weighting values are obtained by assuming that each focus area has the same level of importance. The weight of importance obtained by the AHP approach uses paired comparisons to provide subjective evaluations of factors based on professional considerations and opinions [14]. Based on the weighting values, we calculate the value of cybersecurity awareness in each dimension, focus area, and total weight. Comparisons are carried out using a preference scale, which gives numerical values to various preference level [14].

Table 4. Awareness Criteria

Criteria	Value (%)	Action
Good	77.78 - 100	Action is not needed
Average or Satisfactory	55.56 - 77.77	Action is potentially required
Poor	33.33 - 55.55	Action is required

The score of each focus area and dimensions are calculated and grouped as the awareness criteria in accordance with Table 4. The interval value of criteria is based on the value of the continuum line in which the maximum value is 100% and the minimum score is 33.33% [14]. After calculating the predetermined weights, the results are obtained in the form of cybersecurity awareness criteria in each focus area and dimension. Every result of cybersecurity awareness criterion has actions that need to be carried out at a later stage when cybersecurity awareness is on certain criteria. The result scores for each dimension and focus areas are then grouped as awareness criteria in Table 8.

III. RESULTS AND DISCUSSION

To perform the validity and reliability test of the questionnaire, we used all 400 samples of respondents. Validity test in this research used Product Moment correlation technique. By using the r table value with n = 400 and the significance level of 5%, the r-value of the table obtained is 0.098. The following are the results of the validity tests that have been conducted on the questionnaire.

Table 5. The Results of Cybersecurity Awareness Validity Test

Statement Item	Item Code	Answer		Category
		R. Table	R. Count	
Knowledge_P1	A1.1	0.098	0.529	Valid
Knowledge_P2	A1.2	0.098	0.436	Valid
Knowledge_P3	A1.3	0.098	0.400	Valid
Knowledge_P4	A2.1	0.098	0.418	Valid
Knowledge_P5	A2.2	0.098	0.531	Valid
Knowledge_P6	A2.3	0.098	0.512	Valid
Knowledge_P7	A3.1	0.098	0.265	Valid
Knowledge_P8	A3.2	0.098	0.405	Valid
Knowledge_P9	A3.3	0.098	0.390	Valid
Knowledge_P10	A4.1	0.098	0.572	Valid
Knowledge_P11	A4.2	0.098	0.388	Valid
Knowledge_P12	A4.3	0.098	0.487	Valid
Knowledge_P13	A5.1	0.098	0.571	Valid
Knowledge_P14	A5.2	0.098	0.482	Valid
Knowledge_P15	A5.3	0.098	0.323	Valid
Knowledge_P16	A6.1	0.098	0.388	Valid
Knowledge_P17	A6.2	0.098	0.450	Valid
Knowledge_P18	A6.3	0.098	0.470	Valid
Attitude_P1	B1.1	0.098	0.605	Valid
Attitude_P2	B1.2	0.098	0.438	Valid
Attitude_P3	B1.3	0.098	0.209	Valid
Attitude_P4	B2.1	0.098	0.554	Valid
Attitude_P5	B2.2	0.098	0.449	Valid
Attitude_P6	B2.3	0.098	0.627	Valid
Attitude_P7	B3.1	0.098	0.568	Valid
Attitude_P8	B3.2	0.098	0.431	Valid

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

Statement Item	Item Code	Answer		Category
		R. Table	R. Count	
Attitude_P9	B3.3	0.098	0.536	Valid
Attitude_P10	B4.1	0.098	0.449	Valid
Attitude_P11	B4.2	0.098	0.506	Valid
Attitude_P12	B4.3	0.098	0.414	Valid
Attitude_P13	B5.1	0.098	0.310	Valid
Attitude_P14	B5.2	0.098	0.302	Valid
Attitude_P15	B5.3	0.098	0.559	Valid
Attitude_P16	B6.1	0.098	0.508	Valid
Attitude_P17	B6.2	0.098	0.542	Valid
Attitude_P18	B6.3	0.098	0.517	Valid
Behavior_P1	B1.1	0.098	0.354	Valid
Behavior_P2	B1.2	0.098	0.563	Valid
Behavior_P3	B1.3	0.098	0.197	Valid
Behavior_P4	B2.1	0.098	0.430	Valid
Behavior_P5	B2.2	0.098	0.354	Valid
Behavior_P6	B2.3	0.098	0.413	Valid
Behavior_P7	B3.1	0.098	0.543	Valid
Behavior_P8	B3.2	0.098	0.399	Valid
Behavior_P9	B3.3	0.098	0.540	Valid
Behavior_P10	B4.1	0.098	0.195	Valid
Behavior_P11	B4.2	0.098	0.328	Valid
Behavior_P12	B4.3	0.098	0.267	Valid
Behavior_P13	B5.1	0.098	0.387	Valid
Behavior_P14	B5.2	0.098	0.502	Valid
Behavior_P15	B5.3	0.098	0.294	Valid
Behavior_P16	B6.1	0.098	0.451	Valid
Behavior_P17	B6.2	0.098	0.250	Valid
Behavior_P18	B6.3	0.098	0.320	Valid

The validity test results show that all questionnaire items are valid. Meanwhile, to check the reliability from each items, this research used the Cronbach's Alpha technique with the help of IBM SPSS Statistics 25 software. If r count > r table then the question is declared reliable, if r count ≤ r table then the question is declared unreliable. With a confidence level of 95%, the results are obtained. Cronbach's Alpha coefficient with a minimum value of 0.70 indicates that the questionnaire has a fairly good level of reliability. The following are the results of the reliability tests that have been conducted on the questionnaire.

Table 6. The Results of Cybersecurity Awareness Reliability Test

Cronbach's Alpha	N of Items	Category
0.909	54	Reliable

This research took samples with total 400 respondents in which the questionnaire was distributed by the researcher in January 2020 across Indonesia. The following table is characteristic of the respondents.

Table 7. Respondents' Characteristics by Gender

Sex	Number of respondents	Percentage
Male	46	11.5%
Female	354	88.5%
Total	400	100%

From Table 5, it can be seen that 46 of the total 400 respondents were male respondents (11.5%), and 354 of the 400 respondents were female respondents (88.5%). Based on this data, it can be concluded that female respondents dominated this research.

Table 8. Respondents' Characteristics by Age

Age	Number of respondents	Percentage
18 – 20	203	50.7%
21 – 25	192	48%
26 – 30	4	1%
31 – 40	0	0%
41 – 50	0	0%
> 50	1	0.3%
Total	400	100%

Based on Table 6, out of the 400 samples, total respondents from ages of 18-20 years were 203 respondents (50.7%). Respondents aged 21-25 years were 192 respondents (48%). Respondents aged 26-30 were 4 respondents (2.5%). Respondents aged 31-50 years was 0 respondent (0%). Respondents aged above 50 years was 1 respondent (0.3%). Based on this data, it can be concluded that the age range of 18-28 years dominated the research.

Table 9. Respondents' Characteristics by Regional Domicile

Domicile	Number of respondents	Percentage
Bandung	53	13.25%
Bogor	57	14.25%
Jakarta	43	10.75%
Semarang	21	5.25%

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

Domicile	Number of respondents	Percentage
Surabaya	21	5.25%
Yogyakarta	29	7.25%
Others	176	44%
Total	400	100%

From Table 7, it can be seen that the most respondents who filled out the questionnaire came from Bogor with 57 people (14.3%). Besides Bogor, there were also 53 respondents (13.3%) from Bandung, and another 176 respondents were scattered across Indonesia on "Others" option.

Cybersecurity awareness level is used to present the results and findings obtained from a questionnaire filled out by 400 respondents. Cybersecurity awareness level in Table 8 can provide groupings according to criteria of focus areas that do not require action for improvement, is potentially needing action for improvement, and is requiring action for improvement.

Table 10. Cybersecurity Awareness Level

Focus Area (16.67%)	Dimension			Total awareness/ focus area
	Knowledge (30%)	Attitude (20%)	Behavior (50%)	
Password security	82%	85%	75%	79%
Cyber-bullying	97%	98%	86%	92%
Phishing	79%	82%	77%	78%
Malware	77%	82%	76%	77%
Identity theft	87%	89%	87%	87%
Downloading, sharing, and use of pirated content	79%	75%	53%	66%
Total awareness/ dimension	83%	85%	76%	80%

Based on the cybersecurity awareness level obtained in Table 8, the results according to the dimension are as follows. The total percentage of cybersecurity awareness is 80%. It shows that the level of cybersecurity awareness over dimension is in the good criteria. In this level, the respondents do not need treatment to improve their cybersecurity awareness [14].

The highest percentage of awareness between the three dimension is in the attitude dimension with a percentage of 85%. In this level, the respondents do not need treatment to improve their attitude. The high percentage of 85% is caused by respondents' high tendency to respond positively to cybersecurity topics. Each attitude percentages show a significant amount, and the highest percentage is on questionnaire item B2.2. Questionnaire item B2.2 illustrates that respondents already have good assumptions by considering cyberbullying as an online attack that aims to insult or threaten other people on the internet.

A total percentage of 83% found in the knowledge dimension. In this level, the respondents also do not need treatment to improve knowledge because the percentage is still in the range of good criteria. This happened because according to a survey that had been conducted, the highest percentage out of all knowledge items are on questionnaire items A2.2 and A2.3. These suggest that many of the respondents already have a very good understanding towards the definition of cyberbullying, and respondents are in the state of knowing that intentionally hurting others through social media is the act of cyberbullying.

The lowest percentage is found in the behavior dimension with a total percentage of 76%. This shows that action is potentially required to improve their behavior. From the results of the calculation, it was found that the lowest percentage of behavior items are C1.3, C6.2, and C6.3. This indicates that respondents tend not to change passwords regularly, and there were relatively many respondents who bought and downloaded films illegally, as well as sharing the downloaded files that are illegal with their relatives.

The highest total awareness per focus area is the (b) cyberbullying focus area with a percentage of 92%, followed by (e) identity theft focus area with a percentage of 87%, (a) password security focus area with a percentage of 79%, (c) phishing focus area

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

with a percentage of 78%, (d) malware focus area with a percentage of 77%, and (f) downloading, sharing, and use of pirated content with the smallest percentage of 66%. From the total percentage of each focus area, it can be seen that the focus area of (a) password security, (b) cyberbullying, (c) phishing, and (e) identity theft are all in the good criteria of awareness, and taking action is not fully needed. However, the percentage of (d) malware and (f) downloading, sharing, and use of pirated content show that these focus areas are included in the average criteria, so it can be stated that action is potentially needed for improvement.

Compared to research conducted by Chandarman et al. [15], the focus areas used are the same but the method and objects are different. On Chandarman's research, the method is called Theory of Planned Behavior and the objects are students at a private tertiary education institution in South Africa. There are some similarities found in these two findings. On the research conducted by Chandarman, the responses to cybersecurity attitude questions were compulsive, as students indicated low levels of agreement with the incorrect statements.

Despite of different methods, most students reported the right attitude in regards to content piracy. But at the same time, their actual skills and behavior indicate that they are engaged in content piracy by downloading illegal files. This indicated that students will engage in piracy behaviour even though they know it is wrong. Contrarily, in the case of cyberbullying, most students gave attitude responses that indicated a potentially harmful attitude towards posting images and offensive messages to others. The findings on Chandarman's research also indicate the need for targeted CSA campaigns that overcome the specific weaknesses of specific user population.

Comparing this research with other research conducted by Sari [14], the focus areas, topics, and objects are different. In this research, the object is Indonesian college students but in Sari's research, the object is Indonesian smartphone users. However, the method, dimension, and weightings are the same. There are awareness criteria similarities from this research and the research conducted by Sari. From Sari's research, it was found that knowledge and attitude dimensions exist in a good level of information security awareness. While the behavior dimension is still at an average level. This means that even though they understand about topics related to information security, they don't do as they know in the terms of information security.

IV. CONCLUSION

Based on our research, overall, it is stated that the level of cybersecurity awareness for Indonesian college students is at a good criteria (80%). There are some focus areas that should be addressed in order to have potential improvement. In the knowledge dimension, malware can be addressed and fixed to get a higher percentage. While in the attitude dimension, there is downloading, sharing, and use of pirated content. However in the behavior dimension, there are password security, phishing, malware, and the last is downloading, sharing, and use of pirated content. Based on the results of the study, there are some things that the government and the community can do, especially students, to increase awareness and maintain safe in using the internet such as increasing their knowledge about the purpose of malware, which is related to user's personal data. In addition, users must update their antivirus regularly to avoid cybercrimes. Other than that, possible thing to do by the government and related industries are by holding various programs, socialization, and campaigns related to cybersecurity, especially in terms of content piracy. Because the research data shows that there are still many students who download content illegally even though they know the consequences of content piracy. This study has several limitations. Like the other studies, the respondents involved did not always represent larger population. Also, this research did not always represent other more

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

comprehensive cybersecurity topics. Therefore, for the next research, hopefully the method and framework can be improved with various developments. Such as diverse object, detailed focus area, and deeper qualitative studies in cybersecurity awareness.

REFERENCES

[1] S. Kemp, "Digital 2020: Indonesia", *Data Reportal*, 2020. [Online]. Available: https://datareportal.com/reports/digital-2020-global-digital-overview [Accessed: 26-April-2020]

[2] S. Kemp, "Digital 2019: Indonesia", *Data Reportal*, 2019. [Online]. Available: https://datareportal.com/reports/digital-2019-indonesia [Accessed: 26-April-2020]

[3] Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei APJII yang Ditunggu-tunggu, Penetrasi Internet Indonesia 2018", *Buletin APJII*, edition 40, May 2019. [Online]. Available: https://apjii.or.id/content/read/104/418/BULETIN-APJII-EDISI-40---Mei-2019 [Accessed: 26-April-2020]

[4] M. C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article", *Yale Journal of International Law*, vol. 36, 2011.

[5] A. T. Haryanto, "Ini Bukti Indonesia Rentan Jadi Sasaran Serangan Siber", *DetikInet*, 2019. [Online]. Available: https://inet.detik.com/security/d-4418609/ini-bukti-indonesia-rentan-jadi-sasaran-serangan-siber [Accessed: 28-January-2020]

[6] A. R. Rachmawati, "Kerugian Pembajakan Capai Puluhan Triliun Rupiah Per Tahun", *Pikiran Rakyat*, 2019. [Online]. Available: https://www.pikiran-rakyat.com/ekonomi/pr-01318977/kerugian-pembajakan-capai-puluhan-triliun-rupiah-per-tahun [Accessed: 22-April-2020]

[7] R. Dwinanda, "Lebih dari 500 Ribu Akun Zoom Dijual di Dark Web", *Republika*, 2020. [Online]. Available: https://republika.co.id/berita/q8tm8z414/lebih-dari-500-ribu-akun-zoom-dijual-di-emdark-webem [Accessed: 5-June-2020]

[8] W. Kusuma, "Palsukan Data Diri, Seorang Mahasiswa Kuras Ratusan Juta Uang Temannya di Bank", *Kompas*, 2019. [Online]. Available: https://regional.kompas.com/read/2019/02/26/20300271/palsukan-data-diri-seorang-mahasiswa-kuras-ratusan-juta-uang-temannya-di [Accessed: 26-January-2020]

[9] M. Abdalloh, "40% Serangan Siber Gunakan Malware", *Ayobandung*, 2019. [Online]. Available: https://amp.ayobandung.com/read/2019/11/12/70033/40-serangan-siber-gunakan-malware [Accessed: 26-January-2020]

[10] L. K. Nugraha, and D. A. Putri, Mapping the Cyber Policy Landscape: Indonesia. London: Global Partners Digital, 2016.

[11] Candiwan, P. K. Sari, and N. Nurshabrina, "Assessment of Information Security Management on Indonesian Higher Education Institutions", Advanced Computer and Communication Engineering Technology, vol. 362, 375-385, 2016.

[12] S. Kusumadewi, S. Hartati, A. Harjoko, R. Wardoyo. Fuzzy Multi-Attribute Decision Making (FUZZY MADM). Special Region of Yogyakarta: Graha Ilmu, 2006.

[13] W. V. Sujarweni. SPSS Untuk Penelitian. Special Region of Yogyakarta: PT. Pustaka Baru, 2015.

[14] P. K. Sari, and Candiwan, "Measuring Information Security Awareness of Indonesian Smartphone Users", TELKOMNIKA (Telecommunication Computing Electronics and Control), 12(2), 493, 2014.

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706

[15] R. Chandarman, and B. Van Niekerk, "Students' cybersecurity awareness at a private tertiary educational institution", The African Journal of Information and Communication (AJIC), 20, 133-155, 2017.
[16] H. A. Kruger, and W. D. Kearney, "A Prototype For Assessing Information Security Awareness" Computers & Security, 25(4), 289–296, 2006.

ISSN 2442-7888 (online) DOI 10.24167/sisforma.v7i2.2706