Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 4 October 2024, pp: 1301-1308
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Measuring Information Security Awareness Level of High School Students

Dimas Agung Perkasa[1], Bambang Setiawan[2*]

[1,2]Departemen Sistem Informasi, Fakultas Teknologi Elektro Dan Informatika Cerdas,
Institut Teknologi Sepuluh Nopember, Indonesia

E-Mail: [1]dimasagung14.da@gmail.com, [2]setiawan@is.its.ac.id

Received Jun 12th 2024; Revised Jul 10th 2024; Accepted Jul 20th 2024
Corresponding Author: Bambang Setiawan

Abstract

Information security awareness has become a crucial factor in the current advancement of information technology. Information security awareness is one of the key factors in avoiding crimes in the digital world today. Therefore, this research aims to measure the information security awareness level and provide recommendations to enhance the information security awareness of high school students. The research instrument utilized in this study is the Human Aspect Information Security Questionnaire (HAIS-Q) and focus area weighting was conducted using the Analytic Hierarchy Process (AHP) method. Data was collected through questionnaires distributed to 99 respondents, and the weighting was performed by two experts in the field of information security and one high school teacher. The results indicated a total awareness level of 86,38%, categorized as "Good", with the most vulnerable focus area being password management. Based on these findings, recommendations are provided in this research to enhance information security awareness.

Keywords: AHP, HAIS-Q, High School Students, Information Security Awareness

1. INTRODUCTION

According to a report by We Are Social, the number of internet users in Indonesia in January 2024 reached 185 million, or 66.5% of the Indonesian population. A survey by the Indonesian Internet Service Providers Association (APJII) indicated that the national internet penetration rate in 2024 was 79.5% of the total population. Millennials, or those aged 28-43, ranked first with a penetration rate of 93.17%, followed by Generation Z, or those aged 12-27, with a penetration rate of 87.02%. Generation X and Baby Boomers ranked third and fourth with penetration rates of 83.69% and 60.52% [1].

Based on a survey conducted by Cybersecurity Ventures in 2019, it was estimated that global economic losses due to cyber-attacks would reach $6 trillion by 2021. Therefore, individuals and organizations must have a high awareness of information security. Understanding information security awareness and the factors influencing each individual plays a significant role in mitigating information security [2] Innovations in technology and digital devices bring advantages to an organization's efficiency and productivity, but institutions transitioning to digital also face information security risks. According to the Ministry of Communication and Information Technology Indonesia (Kemkominfo), efforts are needed to enhance data and information security knowledge and awareness among Indonesian teens and young adults. According to Kemkominfo, this can be accomplished through outreach activities, literacy education, and training. Kids and teenagers should also be exposed to programs that improve their understanding and knowledge of data and information security as a basis for their usage of digital media [3]

Cybercriminals have attacked many kinds of private and public entities, including education, banking, healthcare, and other industries [4]. These kinds of businesses possess priceless assets and private employee data. Besides the technical aspect of cybersecurity, the human factor is essential. Studies show that human error contributes to 95% of security breaches, technological security by itself is unable to ensure a safe environment for digital assets within an enterprise [5]. Another definition of information security awareness is the capacity of an individual to comprehend, adhere to, and appropriate security policies, guidelines, and regulations [6]. Enhancing users' security awareness becomes essential for an organization's sustainability. Although there are many variations among organizations and environments, information security awareness has certain standard aspects that aim to secure data and information [7]. As a result, information security awareness must consider how well individuals understand the significance and impact of their behavior on information.

Information security is how we may stop cheating or identify illegal activity. The goal of information security is to protect data assets from potential cyber attacks. Information security awareness is defined as a method to educate internet users to be more vigilant against various types of cyber-crimes and security vulnerabilities in digital device[8]. The rapid growth of information technology also presents new challenges in information security, prompting increased security gaps among information technology user[9]. Building an appropriate level of security awareness among users is crucial for the sustainability of an organization. Information security awareness must also consider the extent to which individuals understand the importance and impact of their behavior on information security [10].

Teenagers increasingly utilize the internet and their devices. They experienced a brief learning curve when it comes to technology. As a result, within this age group, the internet and social media are becoming more and more popular [11]. Technology is becoming an essential component of every teenager's academic experience because of the adoption of digital tools and internet platforms in learning [12]. The growing use of information technology in both daily life and education has made teenagers more vulnerable to the possibility of being exposed to identity theft, cyberbullying, hacking, and online fraud, among various cyber threats [13]. These teenagers often lack the knowledge and awareness required to identify and reduce these risks caused by the shortage of appropriate cybersecurity education. Meanwhile, student's knowledge is essential in maintaining information security [14]. This emphasizes the necessity of extensive cybersecurity training and safety practices in both school environments and home environments [15]. Cybersecurity usually appears as a minor component of computer education in school curricula, and the lack of development and innovation in this curriculum reflects educational institutions' lack of concern about elementary and secondary school teenagers' cybersecurity knowledge and behavior. Lack of emphasis from educational institutions on cybersecurity in the educational curriculum leads to teenagers becoming aware of how to act online from experience, internet instructions, or individuals around them [10].

Research conducted by Kathryn Parsons et al. [16]. still has shortcomings in measuring individual information security awareness using HAIS-Q with only workers in Australia, while research conducted by Jasber Kaur and Norliana Mustafa [17]. only analyzes the influence of knowledge, attitude, and behavior on confidentiality, integrity, and availability in Malaysian SMEs using *partial least squares* analysis and does not measure individual awareness. The last research was conducted by Mainar Swari Mahardika [18], who only measured individual information security awareness among workers at the Judicial Commission Center for Analysis and Information Services, Republic of Indonesia.

Therefore, with the HAIS-Q questionnaire, this study contributes to measuring the information security awareness of high school students in their teenage years. The HAIS-Q questionnaire used in this research is an instrument designed to measure high school students' awareness regarding information security. Based on the measured information security awareness, the results will be utilized in formulating appropriate recommendations to improve high school students' information security awareness.

2. MATERIALS AND METHOD

This research methodology is shown in Figure 1. This research is divided into five stages, namely: 1) building a model, 2) collecting data, 3) processing data, 4) analyzing, and 5) making recommendations.

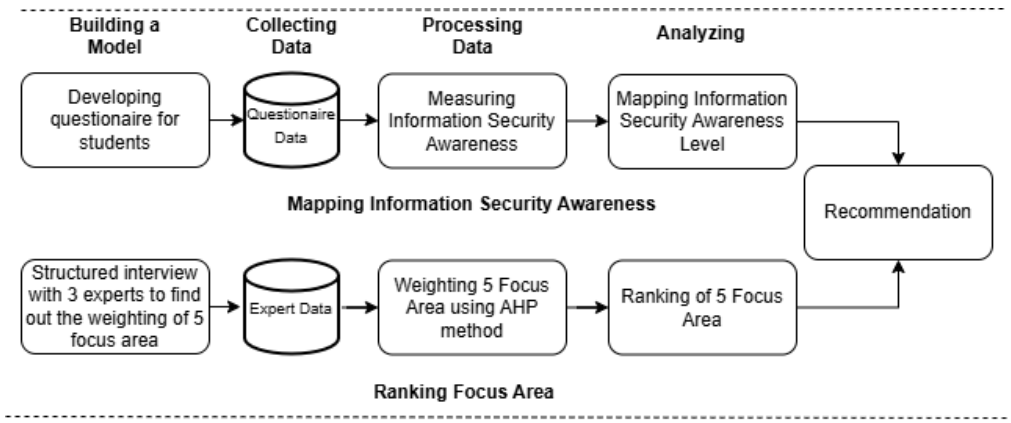

Figure 1. Research Methodology

2.1. Building a Model

This stage was carried out to create a questionnaire of questions for high school students and a structured interview with experts which was used to obtain AHP weighting from three experts. A questionnaire was developed based on HAIS-Q and weighting focus areas using the AHP method.

2.1.1 Developing Questionaire

This research uses quantitative research methods using questionnaire instruments. The questionnaire used in this study refers to the Human Aspect Information Security Questionnaire (HAIS-Q). HAIS-Q has become a questionnaire instrument that can measure an individual's level of concern for data and information security [19]. Questions in the questionnaire were developed from 5 focus areas and 15 sub-areas of HAIS- Q which can be seen in Figure 2.

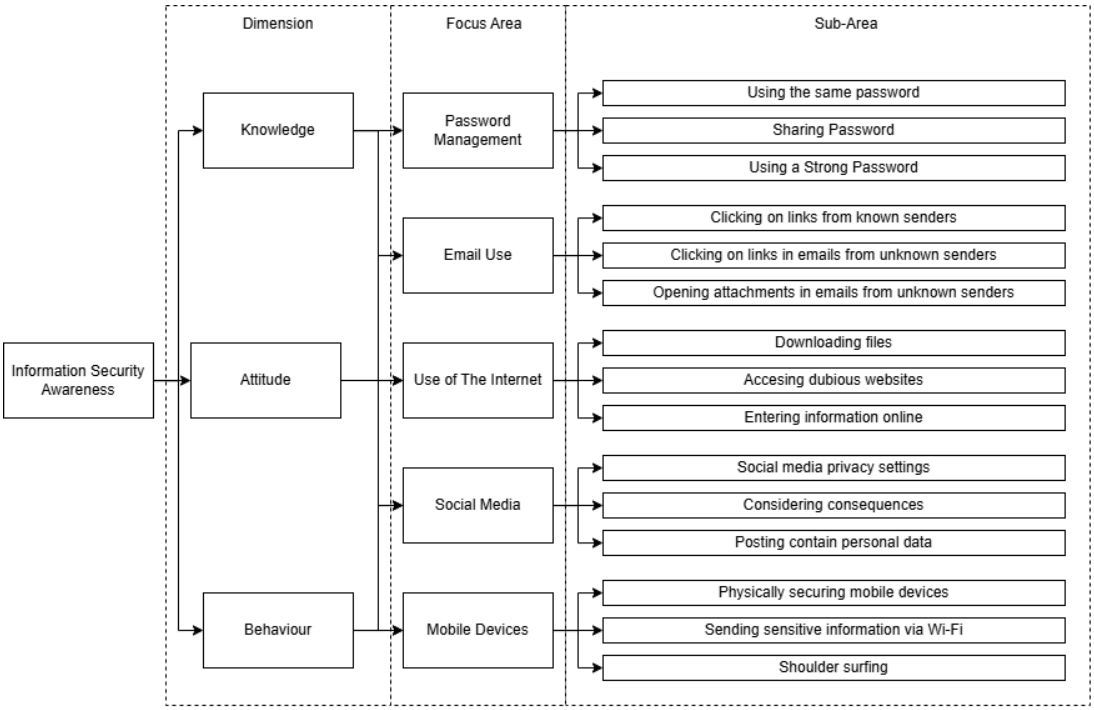

Figure 2. HAIS-Q Focus Area

The respondents of this questionnaire are high school Students in Surabaya, Indonesia. This questionnaire contains two questions regarding the demographics of respondents' gender and age and 45 questions that refer to the HAIS-Q sub-areas and is divided into five sections according to the five focus areas of HAIS-Q. This survey was made with the Google Forms application.

Table 1. Scale of Importance

Intensity of Importance	Definition
1	Equal Importance
2	Equal to Moderate Importance
3	Moderate Importance
4	Moderate to Strong Importance
5	Strong Importance
6	Strong to Very Strong Importance
7	Very Strong Importance
8	Very to Extremely to Strong Importance
9	Extreme Importance

2.1.2 Structured Interview with Expert

Interviews with information systems security experts aim to find the most important focus areas within the five focus areas of HAIS-Q. Interviews were conducted using the AHP method. We used the AHP method in the weighting of this study because the AHP method is suitable for weighting many variables carried out by experts[20]. Interviews were conducted with three experts. Their opinions are filled in a pairwise comparison matrix, as shown in Table 2, to determine the tendency of one focus area to another focus area. The tendency between focus areas is described on a scale of 1-9 with increasing order as seen in Table 2.1.

2.2. Collecting Data

This phase of the study is dedicated to obtaining data. Two types of data are required for this study: high school student information security awareness questionnaire data, which is used to measure their

awareness of information security, and pairwise comparison matrix of expert interview data, which is used to weight the focus area as an input in the AHP.

2.2.1 Questionnaire Data

Questionnaire data was obtained by distributing Google forms to the high school students, from distributing this questionnaire 99 respondents were obtained. These respondents were obtained using a random sampling method distributed to the high school students in Surabaya, Indonesia.

2.2.1 Expert Data

Interviews with experts about students' behavior were conducted with the teachers about current curricula and students' behavior to know more about information security policy and the behavior of the students regarding information security awareness Data obtained from interviews with experts in the form of a pairwise comparison matrix as shown in Table 2.

Table 2. Example of Pairwise Comparison Matrix

	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Email																X		Password Management

The expert will compare the focus areas using a comparison matrix as shown in Table 2. Data from the pairwise comparison matrix is used as input for weighting using the AHP method.

3. RESULTS AND DISCUSSION

3.1. Processing Data

This stage processes the data that has been collected at the data collection stage, the questionnaire data of high school students is processed into the results of measuring the information security awareness of students, and the pairwise comparison matrix data by experts will be processed to determine the weight of each focus area.

3.1.1 Demographics of Respondents

The respondents to this research were high school students from Surabaya. Respondents received a total of 99 questionnaires. Table 3 shows the demographics of 99 respondents, including gender, age, education level, and educational background.

Table 3. Respondents Demographics

Criteria	Variables	Frequency
Gender	Male	49
	Female	50
Age	15	3
	16	39
	17	43
	18	14

Table 3 above shows the demographic of respondents with frequency based on gender, 49 for males and 50 for females. Based on age range from 15, 16, 17, and 18 respectively are 3, 39, 43, and 14.

3.1.2 Result of Measuring Information Security Awareness

The results of the measurement of information security awareness were carried out by calculating the total Likert score of each focus area obtained from the questionnaire data divided by the total maximum score on the focus areas. Table 4 shows the percentage of information security awareness measurement results.

Table 4. Percentage of Information Security Awareness

Focus Area	Knowledge	Attitude	Behavior	Total Awareness
Password Management	84.98%	79.19%	81.75%	81.98%
Email Usage	91.99%	87.21%	88.89%	89.36%
Use of The Internet	91.45%	92.32%	88.28%	89.36%
Social Media	86.20%	82.36%	87.27%	85.27%
Mobile Devices	84.51%	82.42%	86.87%	84.60%
Total	87.82%	84.70%	86.61%	86.38%

Table 4 presents the findings from assessing the information security awareness of students in high schools across five focus areas namely: password management, email usage, use of the internet, social media, and mobile media; and three dimensions namely: knowledge, attitude, and behavior. The level of information security awareness will then be mapped using the analysis of these results.

3.1.3 Weighting Focus Area

The calculation of the pairwise comparison matrix using AHP aims to determine the weight of each focus area based on interviews with three experts. The AHP calculation used AHP calculator tools. We use the weight of this focus area to determine which focus area is the most vulnerable according to experts. Table 5 presents the focus area weight percentage.

Table 5. Focus Area Weight Percentage

Focus Area	Weight (%)
Password Management	29.09%
Email Usage	5.36%
Use of The Internet	8.30%
Social Media	44.14%
Mobile Devices	13.12%
Total Awareness	100%

Table 5 shows the weight in each of the focus areas. These weighting results will then be ranked to know the priority of the focus area.

3.2 Analyzing Data

Following the data processing phase, the data will be analyzed to determine the high school students' awareness of information security and the ranking of the previous focus area weighting using AHP.

3.2.1 Mapping of Information Security Awareness Level

Table 6 presents the mapping of the information security awareness level based on the result of measuring information security awareness in Table 4. The different colors in the table indicate the awareness level of each result. Table 7 explains the meaning of each color.

Table 6. Mapping of Information Security Awareness Level

Focus Area	Knowledge	Attitude	Behavior	Total Awareness
Password Management	84.98%	79.19%	81.75%	81.98%
Email Usage	91.99%	87.21%	88.89%	89.36%
Use of The Internet	91.45%	92.32%	88.28%	89.36%
Social Media	86.20%	82.36%	87.27%	85.27%
Mobile Devices	84.51%	82.42%	86.87%	84.60%
Total	87.82%	84.70%	86.61%	86.38%

The mapping of information security awareness is shown in Table 6. Sequentially, the level of awareness of the dimensions of knowledge, attitude, behavior, and total value in the password management focus area is 84.98%, 79.19%, 81.75%, and 81.98%. In the focus area email usage is 91.99%, 87.21%, 88.89%, and 89.36%. In the focus area use of the internet is 91.45%, 92.32%, 88.28%, and 89.36%. In the social media focus area it is 86.20%, 82.36%, 87.27%, and 85.27%. Meanwhile, the mobile devices focus area is 84.51%, 82.42%, 86.87% and 84.60%.

It can be seen that the lowest value is in the attitude dimension in the password management focus area is the only average level with 79.19%. As for each of the focus areas in each dimension are all at a good level with a percentage above 80%.

Table 7. Level of Awareness

Awareness Level		
Level	Results (%)	Action
Good	80-100	Excellent, no further action required
Average	60-79	Evaluate, possible action required
Poor	0-59	Lacking, further action required

The level of awareness can be categorized into three levels, namely Good, Average, and Poor [21], as shown in Table 7. This level of awareness can be categorized as Good with a result of 80-100%, which means that awareness in the focus area is good, requiring no further action. The Average level with a result of 60-79%

means that awareness in the focus area still needs to be evaluated and possibly needs corrective action. The last one is the Poor level with a result below 59% means that awareness in the focus area is lacking and corrective action must be taken.

3.2.2 Ranking Focus Area

Based on the result of the focus area weight in Table 5. The results of this weight in Table 5 are then ranked from the largest to the smallest weight to find out which focus area is the most vulnerable focus areas. The ranking of the focus area weights can be seen in Table 8.

Table 8. Focus Area Ranking

Focus Area	Weight (%)	Rank
Social Media	44.14%	1
Password Management	29.09%	2
Mobile Device	13.12%	3
Use of The Internet	8.30%	4
Email Usage	5.36%	5

From Table 8, we can see that the rank of the most important focus areas according to experts are social media with a weight percentage of 44.14%, password management at 29.09%, mobile devices at 13.12%, use of the internet at 8.30%, and the last is email usage with 5.36%.

3.3 Recommendation

According to the results of Table 4, it can be said that the student's concern for information security is at the "Good" level, indicated by 23 green boxes indicating the "Good" level. Comparing Table 7 of the focus area weight ranking with Table 4 of the results of measuring information security awareness, it can be analyzed that the focus area of password management needs more attention. The attitude of password management is 79,19%, which is the only "Average" level, and the focus area of password management occupies a weighting ranking at number 2. Therefore, according to research conducted by Mahardika [5] the right recommendation to increase student awareness of information security, especially in the focus area of password management is as follows:

1. The institutions or schools can make banners or posters that remind students that a good password must consist of at least 8 characters long and include numbers, symbols, capital letters, and also lowercase letters.
2. The teachers can always remind the students not to share their passwords, and not to use the same password for many accounts.
3. Provides knowledge of information security standards that follow ISO 27001. The recommendation is to enhance the level of the entire focus area.
4. The school educates teachers and people on information security standards that follow ISO 27001. This recommendation will enhance information security awareness throughout all target areas.

Increasing information security awareness also needs socializing and training for students regarding information security, which is critical for educational institutions. The way to socialize information security can be in various ways, For instance:

1. Socialization by sending WhatsApp messages to student groups.
2. Socialization of information security through banners and brochures.
3. Socialization by holding seminars or workshops on information security attended by all students.

Socialization can also be done by adopting habits based on other organizations or institutions that have successfully carried out good information security habits. Management or leaders can also set an example and participate in monitoring to maintain the level of information security awareness at the schools.

4. CONCLUSION

The findings of measuring the students' awareness level of information security show results at the "Good" level. This condition shows that the majority of students of high school in Surabaya are aware of the importance of information security. The results of measuring awareness using HAIS-Q and the results of weighting focus areas by experts in the field of information security show that the most vulnerable focus area is the focus area of password management.

This research provides recommended solutions to schools to increase the level of information security awareness of students. The recommended recommendation is the need for a policy in educational institutions regarding information security that refers to the ISO 27001 information security standard. This research provides recommended solutions to schools to increase the student's level of information security awareness.

The recommended recommendation is the need for policies in educational institutions regarding information security that refer to the ISO 27001 information security standard. This research also provides recommendations for the need for intensive activities to socialize information security policies implemented by schools to students.

These findings imply that we contribute to knowing the level of teenagers or high school students' awareness of information security because the previous research measured the awareness of adults or workers in an enterprise, such as workers in judicial commissions, workers in Australia, and workers in SMEs in Malaysia. Therefore, this study is necessary to know teenagers' awareness to improve teenagers' awareness so that when they become adults, they already have improved information security awareness. For future research, we can apply the recommendations from this research and then measure them again to know how impactful these recommendations are in improving students' awareness of information security.

REFERENCES

[1] Cindy, "Penetrasi Internet Generasi Milenial Tertinggi Dibanding Kelompok Usia Lainnya di Indonesia."

[2] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Comput Secur*, vol. 88, Jan. 2020, doi: 10.1016/j.cose.2019.101640.

[3] V. A. Tandirerung, R. T. Mangesa, and Syahrul, "published-teknovokasi-vol1-no2-Veronika-Asri," *TEKNOVOKASI: Jurnal Pengabdian Masyarakat*, vol. 1, no. 2, 2023.

[4] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, Mar. 2023, doi: 10.1016/j.heliyon.2023.e14234.

[5] T. Rahman, R. Rohan, D. Pal, and P. Kanthamanon, "Human Factors in Cybersecurity: A Scoping Review," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jun. 2021. doi: 10.1145/3468784.3468789.

[6] K. Firsty Arisya, Y. Ruldeviyani, R. Prakoso, and A. Lailatul Fadhilah, "Measurement of information security awareness level: A case study of mobile banking (m-banking) users," in *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/ICIC50835.2020.9288516.

[7] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput Secur*, vol. 106, Jul. 2021, doi: 10.1016/j.cose.2021.102267.

[8] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," *Journal of Computer Information Systems*, vol. 60, no. 3. Taylor and Francis Inc., pp. 201–211, May 03, 2020. doi: 10.1080/08874417.2018.1432996.

[9] A. Tolah, S. M. Furnell, and M. Papadaki, "An empirical analysis of the information security culture key factors framework," *Comput Secur*, vol. 108, Sep. 2021, doi: 10.1016/j.cose.2021.102354.

[10] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the Netherlands," *Comput Educ*, vol. 186, Sep. 2022, doi: 10.1016/j.compedu.2022.104536.

[11] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30. Elsevier B.V., Dec. 01, 2021. doi: 10.1016/j.ijcci.2021.100343.

[12] A. Haleem, M. Javaid, M. A. Qadri, and R. Suman, "Understanding the role of digital technologies in education: A review," *Sustainable Operations and Computers*, vol. 3, pp. 275–285, Jan. 2022, doi: 10.1016/j.susoc.2022.05.004.

[13] A. W. Fazil, M. Hakimi, S. Sajid, M. M. Quchi, and K. Q. Khaliqyar, "Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province," *American Journal of Education and Technology*, vol. 2, no. 4, pp. 50–61, Nov. 2023, doi: 10.54536/ajet.v2i4.2248.

[14] N. A. Prasetyo and B. Setiawan, "Kajian Dimensi Budaya Keamanan Informasi dalam Berbagai Organisasi," *JTERA (Jurnal Teknologi Rekayasa)*, vol. 7, no. 1, p. 73, Jun. 2022, doi: 10.31544/jtera.v7.i1.2022.73-82.

[15] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378–382, May 2020, doi: 10.18178/ijiet.2020.10.5.1393.

[16] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput Secur*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.

[17] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," in *International Conference on Research and Innovation in Information Systems, ICRIIS*, 2013, pp. 286–290. doi: 10.1109/ICRIIS.2013.6716723.

[18] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, "Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 3, pp. 501–509, Jun. 2020, doi: 10.25046/aj050362.

[19] S. N. Kamaruzzaman, E. C. W. Lou, P. F. Wong, R. Wood, and A. I. Che-Ani, "Developing weighting system for refurbishment building assessment scheme in Malaysia through analytic hierarchy process (AHP) approach," *Energy Policy*, vol. 112, pp. 280–290, Jan. 2018, doi: 10.1016/J.ENPOL.2017.10.023.

[20] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," *Procedia Comput Sci*, vol. 234, pp. 1396–1403, Jan. 2024, doi: 10.1016/J.PROCS.2024.03.138.

[21] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput Secur*, vol. 25, no. 4, pp. 289–296, Jun. 2006, doi: 10.1016/j.cose.2006.02.008.