IRJEMS International Research Journal of Economics and Management Studies
Published by Eternal Scientific Publications
ISSN: 2583 – 5238 / Volume 3 Issue 6 June 2024 / Pg. No: 354-361
Paper Id: IRJEMS-V3I6P139, Doi: 10.56472/25835238/IRJEMS-V3I6P139

Original Article

Examining the Knowledge, Attitude, and Behavior of IT Division Staff on Information Security Issues: A Case Study in a Telecommunication Company

[1]Maudhita Ramadhani, [2]Puspita Kencana Sari
[1,2] School of Economics and Business, Telkom University, Bandung, Indonesia.

Received Date: 21 May 2024 Revised Date: 07 June 2024 Accepted Date: 16 June 2024 Published Date: 26 June 2024

Abstract: *In the digital age, information security has become important to the success of many enterprises and individuals. However, the increasing growth of the telecommunications industry creates possible threats for these businesses. It is indisputable that human resources, particularly those in the Information Technology (IT) Division, play an important role in information security. The purpose of this study is to examine information security awareness levels using the Human Aspects of Information Security Questionnaire (HAIS-Q), which includes three dimensions: knowledge, attitude, and behavior. The study looked at seven main areas that represent contemporary information security risks in the firm. This study examines a telecommunications business in Indonesia and collects data from a survey of IT Division employees as a sample. The results show a high degree of information security knowledge across all dimensions and areas. However, the behavior has the lowest level, especially in terms of email usage and mobile device concerns.*

Keywords: *Information security, security awareness, Security Education Training Awareness* (SETA), *HAIS-Q.*

I. INTRODUCTION

Information security is a protection against a risk of information that can threaten the integrity of the information [1]. Security information was also to protect computers, facilities, data, and information from abuse by irresponsible persons [2]. In this context, information security awareness is control regulations created with the purpose of reducing the violation of information security caused by negligence and the act of planning [1]. Awareness and understanding someone about security information and action should be taken to protect information from security threats [3]. Threat security trends will be a useful source of information to improve understanding of cybersecurity culture among various organizations with an interest in cybersecurity. AT&T, the world's largest telecommunication company in the US, has been breached where personal data belonging to 73 million active and inactive AT&T customers had been leaked and published on the dark web [4]. In another case, a subsidiary of the German telecommunications giant known as T-Mobile had a history of data leaks in November 2022 that led the telecommunications service provider to agree to pay $150 million for data protection and cybersecurity. Previously, T-Mobile reported breaches in January 2021, November 2019, and August 2018. In Indonesia, the most frequent security incidents for individuals, agencies, and organizations are data breaches at 26%, followed by web defacement incidents at 26%, and Ransomware at 24% [5]. It can be concluded that ransomware and data breach are problems that must be watched because they will be the main spotlight in the cyber threat prediction.

PT ABC, a telecommunications network company in Indonesia that provides a variety of services, including telephony, internet, and cloud, has experienced data leaks. After a thorough investigation, the company discovered that the leaked data was fabricated and misused by irresponsible parties. This incident became a warning to the company about the importance of maintaining data security and customer privacy. As a Telecommunication company that is closely involved in managing information systems for public services, PT ABC realizes the importance of maximizing security awareness, especially within the Information Technology (IT) division that is responsible for ensuring the protection of sensitive data.

Finding information security priority areas that still require improvement is one way to gauge the level of awareness regarding information security. Information security awareness is measured using The Knowledge-Attitude-Behavior (KAB) theory and the Analytic Hierarchy Process (AHP) paradigm because of its benefits for decision-making and capacity to consider both quantitative and qualitative features [6]. AHP makes sure that qualitative and quantitative variables can be assessed simultaneously by taking decision-makers priorities into account [7]. Human Aspects of Information Security Questionnaire (HAIS-Q) is an instrument that can predict information security behavior, making it a measurement tool for security awareness, including knowledge, attitudes, and behaviors to evaluate information security awareness [8]. Previous research [9] has confirmed that HAIS-Q is an effective instrument for measuring information security awareness and outlines

how organizations can improve information security. HAIS-Q can measure information security awareness in employees. Previous research [10] measured the level of information security awareness among Mobile Banking (M-Banking) users in Indonesia. The results of the study state that the AHP method helps in choosing the best option from several alternatives by considering various relevant factors and criteria. Based on this explanation, this study will assess employees' knowledge, attitudes, and behaviors related to data safety using HAIS-Q instruments and AHP as a data analysis technique.

This research's objectives are to assess the knowledge, attitude, and behavior of PT ABC IT division staff in PT ABC regarding information security and offer suggestions for raising their awareness of PT ABC. This research is crucial because the company's information system is an important asset that must be protected from security threats, such as cyber-attacks, data breaches, and data misuse. The IT division is responsible for managing and securing the company's information systems. The IT division has a deep understanding of information technology, access to the data and resources needed, and responsibility for ensuring the security of the company's information systems. The study proposes a theoretical contribution to the future development of HAIS-Q as a measurement model to describe information security awareness, specifically for the telco industry. As practical implications, this study can help PT ABC to improve their IT staff's security awareness following the implementation of security education and awareness campaigns in the company. This study is organized into the following sections: an introduction that provides background information on the topic selection, a research methodology that details the methodology employed results and a discussion section that includes an explanation of the research results and research conclusions.

II. LITERATURE REVIEW

A) Information security awareness

Information security is the protection of information against risks that can threaten the integrity of information confidentiality [1]. Information security is also to prevent the misuse of facilities, data, knowledge, and computer and non-computer equipment by irresponsible persons [2]. Information security awareness is a control/regulation created with the aim of reducing the incidence of breaches to information security caused by negligence or planning actions [3]. A person's awareness and understanding of the importance of information security and the actions that must be taken to protect that information from security threats [11]. Security Education, Training, and Awareness (SETA) program is one way to increase users' information security awareness and develop individual capabilities in dealing with cybersecurity threats [12]. The SETA program aims to protect information assets in an organization by providing knowledge, training, and awareness of information security threats and information system security to employees. The SETA program also aims to raise staff members' understanding of their obligations in safeguarding the company's information assets [9].

B) Human Aspect of Information System Questioner (HAIS-Q)

HAIS-Q is an instrument that can be used to assess the knowledge, attitudes, and behaviors of employees, also known as the KAB element. This component of KAB is a standard that can help organizations address various problems [13]. HAIS-Q is a framework that covers a wide range of information security practices [14]. HAIS-Q can predict information security behavior, making it a valuable tool for information security practitioners. The primary element or instrument of HAIS-Q is an accuracy-verified questionnaire designed to gauge attitudes, knowledge, and beliefs around information security. Knowledge, Attitude, and Behavior (KAB) are the three variables that make up the HAIS-Q measuring methodology. It was determined to evaluate the knowledge (what you know), attitude (what you think), and action (what you do) aspects as a preliminary segmentation of what to test [15].

III. RESEARCH METHODS

This research uses a quantitative research method. We adapted a research framework from previous research [16] that combines the KAB dimensions and the seven focus areas that refer to information security issues involving employees [17]. Managing passwords, email, the internet, social media, mobile devices, data handling, and incident reporting make up the focal area. From ideas, data, and occurrences pertaining to data safety in Indonesia's telecommunications industry, seven key topics were identified [16]. The focus area of protecting personal data passwords was taken up for analysis in this study because people store a lot of information on their devices, including personal and confidential data. They use their devices not only to send messages and make phone calls but also to conduct business via email. The threat of spamming through the web can be caused by the installation of mobile applications on smartphones as well as the use of the internet. The next area of focus is data handling and incident reports, employees must maintain data information because they use devices for business and many other purposes and report incidents such as viruses, theft, and loss [18].

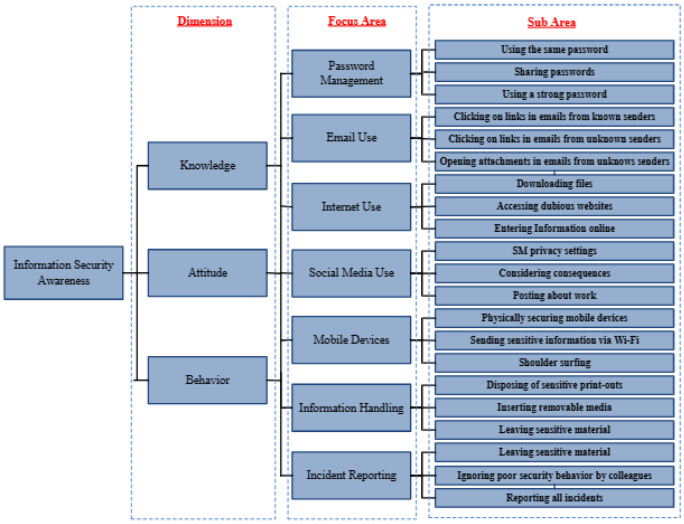

Figure 1. Conceptual Framework

Source: *Parsons et al., 2017*

The data collection was conducted by distributing questionnaires to employees of PT ABC Information Technology Division through Google Forms. Respondents' answers were assessed using a nominal scale by labeling the answers "No" as 1 (one), "Don't Know" as 2 (two), and "Yes" as 3 (three). Figure 1 shows how the HAIS-Q framework is utilized to evaluate staff members' awareness of data safety. The Analytical Hierarchy Process (AHP) is used to analyze information by evaluating the parameters that were determined and focal regions. Based on their level of importance [19]. Several criteria that are compared with each other (the level of importance) are the main emphasis on the AHP concept [20]. AHP's multi-criteria decision-making method is used to determine the weight of factors that affect risk. This method allows experts to assess risk factors qualitatively and quantitatively and then assign weight to each factor based on its importance. This method is used to overcome complexity in decision-making by outlining a hierarchy of dimensions and sub-dimensions that need to be improved in information security awareness [17]. The AHP is used to determine the scale of awareness by providing a judgment-based subjective assessment of the components through pairwise comparisons. The point total for every dimension's focus area was calculated and then normalized to a sum of one determined using the formula below [21]. Vi(a) is obtained based on a questionnaire prepared with as many as 27 questions used to test the knowledge, attitude and behavior of participants related to the seven areas of information security.

$$V(a) = \sum_{i=1}^{n} Vi\,(a)Wi$$

Description:
V(a) = the value of all alternatives,
Vi(a) = the score value that represents each alternative,
Wi = the weight given to describe the level of importance of the criteria obtained using the AHP method

Dimensions weighting (see Table 1) has been determined based on its level of importance refers to the weighting of Kruger & Kearney (2006) [22]. This decision was taken because the behavioral aspect is considered to have a more significant impact on the way individuals deal with information security issues. Meanwhile, the knowledge dimension is given greater weight compared to the attitude dimension because knowledge allows users to influence the way they behave. Since the company gives the same priority to security issues in the focus area, the weighting will be separated equally. We categorize the level of information security awareness in each focus area as Good, Average, and Poor, referring to the previous study [18]. The categories include Good, with a percentage range of 77.7% to 100%; average, with a percentage range of 55.5% to 77.7%; and Poor, with a percentage range between 33.3% to 55.5%.

Table 1: Dimension Weighting

Dimension	Weight
Knowledge	30%
Attitude	20%
Behavior	50%

III. RESULTS AND DISCUSSION

A) Respondent Characteristic

The population of this study were IT division employees of PT ABC. The total of participants in this study amounted to 100 respondents. Table 2 displays the demographics of the participants.

Table 2: Respondent Characteristics

Profile	Category	Frequency	(%)
Gender	Male	64	64%
	Female	36	36%
Age	24 – 30 years	59	59%
	30 – 40 years	28	28%
	> 40 years	13	13%
Education Level	Under-graduate	69	69%
	Graduate	31	31%
Job Position	Manager	8	8%
	Officer	41	41%
	Administrator	24	24%
	Others	27	27%

B) Measurement Model Analysis

The measurement of validity analysis using SPSS 25.0 for the window. The findings of this validity analysis are presented below, and the r-table value is 0.361. The validity test will be calculated using the significance level with the following criteria: (1) The inquiry is valid if r count > r table; (2) the inquiry is invalid if r count < r table. All the items are valid and suitable for usage for additional measurements, according to the results of the validation examination (Table 3).

Table 3: Validity Analysis

Factor	Code	R Count	Description
Knowledge	K1	0.656	Valid
	K2	0.683	Valid
	K3	0.594	Valid
	K4	0.678	Valid
	K5	0.635	Valid
	K6	0.669	Valid
	K7	0.721	Valid
	K8	0.571	Valid
	K9	0.814	Valid
	K10	0.607	Valid
	K11	0.695	Valid
	K12	0.866	Valid
	K13	0.599	Valid
	K14	0.601	Valid
	K15	0.571	Valid
	K16	0.809	Valid
	K17	0.813	Valid
	K18	0.668	Valid
	K19	0.774	Valid
	K20	0.625	Valid
	K21	0.608	Valid
Attitude	A1	0.627	Valid
	A2	0.660	Valid
	A3	0.481	Valid
	A4	0.624	Valid

	A5	0.589	Valid
	A6	0.517	Valid
	A7	0.718	Valid
	A8	0.718	Valid
	A9	0.753	Valid
	A10	0.746	Valid
	A11	0.727	Valid
	A12	0.785	Valid
	A13	0.683	Valid
	A14	0.700	Valid
	A15	0.776	Valid
	A16	0.709	Valid
	A17	0.585	Valid
	A18	0.620	Valid
	A19	0.647	Valid
	A20	0.733	Valid
	A21	0.703	Valid
Behavior	B1	0.661	Valid
	B2	0.704	Valid
	B3	0.711	Valid
	B4	0.726	Valid
	B5	0.812	Valid
	B6	0.660	Valid
	B7	0.674	Valid
	B8	0.580	Valid
	B9	0.731	Valid
	B10	0.801	Valid
	B11	0.775	Valid
	B12	0.649	Valid
	B13	0.797	Valid
	B14	0.737	Valid
	B15	0.761	Valid
	B16	0.844	Valid
	B17	0.509	Valid
	B18	0.549	Valid
	B19	0.820	Valid
	B20	0.773	Valid
	B21	0.665	Valid

The idea of reliability is the capacity to utilize an object as a data-gathering tool with confidence because it has demonstrated its effectiveness. A statistic which is frequently utilized to assess the dependability of an instrument for study is Cronbach's alpha coefficient (□□). When the study instrument's Cronbach's Alpha coefficient is above or equal to 0.70, it is considered to have a sufficient level of reliability [23]. Table 4 shows that all variables are reliable categories since the coefficient is > 0.70.

Table 4: Reliability Analysis

Factor	**Cronbach's Alpha**	**N of Items**
Knowledge	0,938	21
Attitude	0,936	21
Behavior	0,949	21

C) Data Analysis

The data were calculated using the AHP method to determine whether the results fall into the good, average, or poor categories. Based on Table 5 shows that the three indicators are in the average category, namely Email usage, Internet usage, and Mobile equipment. Meanwhile, the others are in the good category.

Table 5: Measurement of Total Awareness

Focus Area	Dimension			Awareness
	K	A	B	
Password Handling	96,67%	100%	80%	89,00%
Email Usage	90,78%	70%	64,78%	73,59%
Internet Usage	98%	99%	72%	85,20%
Social Media Usage	99%	96%	99,44%	98,62%
Incident Report	97,89%	96,56%	95,11%	96,16%
Mobile Equipment	77%	71,56%	79,56%	77,19%
Data Handling	96,78%	97,33%	80%	88,46%
Total Awareness	**93,73%**	**90,06%**	**81,56%**	**86,89%**

D) Discussion

a. Information Security Awareness Level

The result shows the level of information security awareness in IT division staff PT. ABC, which consists of knowledge, attitude, and behavior dimensions, can be described as steadfast and does not take an act. However, there are some areas that need to be improved to prevent the risk as they have lower measurement scores. First, there is an issue with email usage at the lowest level of awareness. This suggests that there are still employees who open or forward email messages from suspicious sources. Supervision should be provided to employees to be more vigilant against phishing attacks and viruses. The second area with the lowest focus is mobile device security. These findings reveal that employees lack understanding and awareness when it comes to securing electronic devices, such as connecting personal devices to company equipment and transmitting sensitive information over public Wi-Fi. Supervision is necessary for employees who fail to securely send files when connected to a network, whether public or private. Lastly, internet usage has the lowest score in the behavior dimension despite a good overall score. This indicates that some employees still access questionable websites. The company needs to enhance employee practices, particularly in regard to avoiding fraud on websites.

Based on the study results, it can be concluded that the respondents' level of security awareness in terms of knowledge is good. This is supported by the highest average level of security awareness, aligning with previous research [21] indicating that knowledge has the highest awareness level at the Information Analysis and Services Centre, Judicial Commission of the Republic of Indonesia. Overall, respondents' security awareness in the knowledge aspect is good, but there are areas, like mobile equipment, that still require improvement. Respondents' security awareness in the attitude dimension is at a good level as a whole. The research aligns with a study [24] that focuses on email usage, particularly in opening suspicious phishing emails from forged senders on cellular and device-linked sub-areas. Overall, respondents' security awareness in terms of behavior is at a good level. Despite this, there are specific areas that require improvement, such as email usage, internet usage, and mobile device security. Interestingly. These findings contrast with the previous research [25], which indicated that behavioral aspects had the highest level of awareness when measuring information security and privacy awareness among Android smartphone users in Indonesia.

b. The Pattern of Information Security Awareness

Figure 2 represents the relationship between knowledge, attitude, and behavior as dimensions of information security awareness. The higher the value, the greater the level of awareness in a particular dimension. This graph shows a positive correlation between the 3 dimensions of information security awareness and the awareness value of each of the 7 indicators.

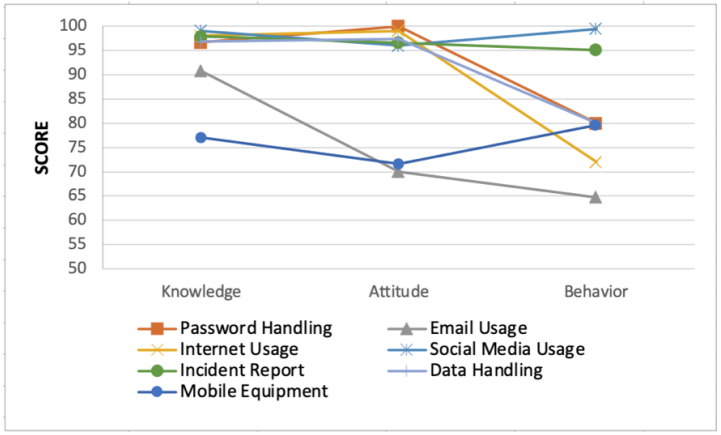

Figure 2. Relations among Knowledge-Attitude-Behavior

The orange-square line represents employees' knowledge of password management. The cross-yellow line represents employees' awareness and knowledge of internet usage. The single strip-blue line represents employees' awareness and knowledge of data handling along the system usage and maintenance. All the lines indicate a slight increase in the attitudes of employees, highlighting the crucial role of a strong security culture in enhancing overall awareness. On the behavior front, there has been a significant decrease. This suggests that when employees are educated on password handling, Internet usage, and data handling policies, procedures, and practices, they are more inclined to focus on knowledge and attitudes over actual security measures, potentially increasing the risk of cyberattacks. However, these trends generally happen in information security awareness studies where knowledge would be the lowest level among other dimensions.

Meanwhile, the triangle-grey line that represents employee awareness of email usage shows an unstable line. It shows a decline not only in employee behavior but also in attitudes. This trend indicates that employees are less aware of understanding and implementing the protection of email according to employee procedures.

The circular blue line representing employee awareness of mobile equipment displays a different pattern. It resembles the star blue line that signifies awareness of social media usage. Both lines indicate a slight decrease in employees' attitudes towards device usage, but there is a noticeable increase in emphasis on the behavioral dimension repeatedly demonstrated by employees. This suggests that employees may not fully agree with policies and procedures on social media and mobile device usage, but they are actively taking steps to protect their accounts and equipment. The circle-green line signifies the level of employee awareness of incident reporting within the company, which is currently at a good level. Despite a slight decline in attitude and behavior, this awareness remains more stable compared to other areas of focus. Employees' high knowledge of cybersecurity threats and incidents supports their positive attitude and good practice in reporting incidents to the relevant parties.

The increasing trend of the awareness score line indicates a positive correlation between different dimensions of information security awareness. Strengthening awareness in each dimension leads to a better understanding of cybersecurity issues overall. This emphasizes the necessity of a comprehensive approach to information security awareness encompassing all dimensions. The diagram effectively demonstrates how interconnected various indicators of information security awareness are and their combined influence on cybersecurity knowledge, attitudes, and behaviors.

IV. CONCLUSION

The degree of awareness of data security among IT Division Employees in PT ABC is "good" and does not need significant assistance. However, it is preferable to give monitoring so that staff are more alert and concerned about the information security of firm data. It would be preferable to focus on the mobile equipment issue because many employees continue to unconsciously connect their devices to office devices, use email by opening messages from unknown people, and send sensitive files while connected to public networks (free Wi-Fi), all of which have the potential to jeopardize the security of personal and business information. Furthermore, the email usage indication indicates that respondents have a low attitude knowledge of normal email usage methods, as seen by the fact that some employees continue to open email messages from unknown persons. As a result, PT ABC must build a work environment that enforces rigorous security standards and increases employee commitment to security behavior by rewarding workers who demonstrate excellent security behavior. The organization must also acknowledge personnel who have demonstrated information security understanding. This system can offer feedback to employees who have completed training to help them regularly follow the regulations. It is meant to serve as an example to employees who are not yet aware of the company's aims, motivating them to attain them. This is possible because rewarding is the most crucial component in the learning process for achieving goals like character development or behavior modification, which must be repeated until it becomes a habit. For future study, it is vital to measure things other than IT divisions that rely heavily on data security. Furthermore, future studies can employ other methodologies, such as qualitative, to gain a deeper understanding of information awareness. Future studies might possibly employ different dimensions or measuring devices to provide a new viewpoint.

V. REFERENCES

[1] M. E. Whitman and H. J. Mattord, *Management of information security*. Cengage Learning, 2018.
[2] P. K. Sari and N. Trianasari, "Information security awareness measurement with confirmatory factor analysis," in *International Symposium on Technology Management and Emerging Technologies*, 2014, pp. 218–223. doi: https://doi.org/10.1109/ISTMET.2014.6936509.
[3] S. P. Sari, A. R. Yunita, F. E. Putri, D. S. Felissia, Y. R. Fadhillana, and N. Z. Arizzal, "Hukum Perdata Nasional di Era Digital: Tantangan dan Peluang Dalam Perlindungan Data Pribadi," in *Proceeding of Conference on Law and Social Studies*, 2023, vol. 4, no. 1.
[4] S. Seddon, "AT&T data breach: Millions of customers caught up in major dark web leak," *BBC News*, 2024. https://www.bbc.com/news/world-us-canada-68701958 (accessed Jun. 15, 2024).
[5] BSSN, "Berita Edukasi Siber," *Badan Siber dan Sandi Negara*, 2023. https://www.bssn.go.id/ (accessed Jun. 15, 2024).
[6] N. D. Ersoz, S. Demir, M. Dilman Gokkaya, and O. Aksoy, "Prioritizing user preferences for quasi – Public space by using analytic hierarchy process (AHP): bursa Podyum park, Turkey case," *Open House Int.*, Jan. 2024, doi: 10.1108/OHI-04-2023-0076.
[7] D. S. Ilcev, "Design and Types of Wire Mobile Satellite Antennas (MSA)," *J. Marit. Res.*, vol. 20, no. 2, pp. 1–5, 2023, [Online]. Available:

https://www.jmr.unican.es/index.php/jmr/issue/view/69

[8] R. Fadlika, Y. Ruldeviyani, Z. T. Butarbutar, R. A. Istiqomah, and A. A. Fariz, "Employee Information Security Awareness in the Power Generation Sector of PT ABC," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, 2023, [Online]. Available: www.ijacsa.thesai.org

[9] 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, 2017, doi: https://doi.org/10.1016/J.COSE.2017.01.004.

[10] K. F. Arisya, Y. Ruldeviyani, R. Prakoso, and A. L. Fadhilah, "Measurement of information security awareness level: A case study of mobile banking (m-banking) users," in *2020 Fifth International Conference On Informatics And Computing (Icic)*, 2020, pp. 1–5. doi: https://doi.org/10.1109/ICIC50835.2020.9288516.

[11] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022.

[12] A. Alyami, D. Sammon, K. Neville, and C. Mahon, "Keberhasilan kritisfaktor untukKeamanan Pendidikan, Pelatihan Dan Kesadaran (SETA) program keefektifan: Alingkaran kehidupan model," *Inf. Teknol. Rakyat*, vol. 36, no. 8, pp. 94–125, 2023, doi: doi: https://doi.org/10.1108/ITP-07-2022-051.

[13] M. A. Fauzi, P. Yeng, B. Yang, and D. Rachmayani, "Examining the link between stress level and cybersecurity practices of hospital staff in Indonesia," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–8.

[14] Nugeraha, "Analytical Hierarchy Process (AHP)," 2017. [Online]. Available: https://repository.nusamandiri.ac.id/index.php/unduh/item/6014/File_15-BabII-Landasan-Teori.pdf

[15] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017b). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/J.COSE.2017.01.004

[16] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006.

[17] Y. A. Styoutomo and Y. Ruldeviyani, "Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001: 2013: A Case Study of XYZ Financial Institution," *CommIT (Communication Inf. Technol. J.*, vol. 17, no. 2, pp. 133–149, 2023, doi: https://doi.org/10.21512/commit.v17i2.8272.

[18] P. K. Sari and C. Candiwan, "Measuring information security awareness of Indonesian smartphone users," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 12, no. 2, pp. 493–500, 2014.

[19] J. Zhao, Y. Zhou, and L. Shuo, "A situation awareness model of system survivability based on variable fuzzy set," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 8, pp. 2239–2246, 2012.

[20] C.-C. Wu, C.-C. Ho, and K.-C. Yang, "Selecting indicators of acupuncture service quality using analytic hierarchy process," *Eur. J. Integr. Med.*, vol. 66, p. 102324, 2024.

[21] M. Amin, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda) Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda)," *J. Penelit. Dan Pengemb. Komun. Dan Inform. Vol*, vol. 5, no. 1, 2014.

[22] M. Mahardika, A. Hidayanto, P. Agya, L. 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," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, no. 3, pp. 501–509, Jan. 2020, doi: 10.25046/aj050362.

[23] Arikunto, S. (2018). Prosedur Penelitian: Suatu Pendekatan Praktik. Rineka Cipta.

[24] A. Zulfia, R. Adawiyah, A. N. Hidayanto, and N. F. A. Budi, "Measurement of employee information security awareness using the human aspects of information security questionnaire (HAIS-Q): Case study at PT. PQS," in *International Conference on Computing Engineering and Design (ICCED)*, 2019, pp. 1–5.

[25] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018.