Employee Information Security Awareness in the Power Generation Sector of PT ABC

Ridwan Fadlika[1], Yova Ruldeviyani[2], Zenfrison Tuah Butarbutar[3],
Relaci Aprilia Istiqomah[4], Achmad Arzal Fariz[5]
Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia[1,2,3,4,5]

***Abstract*—Presidential Regulation No. 82 of 2022 demonstrates the Indonesian government's dedication to protecting Vital Information Infrastructure, which has become increasingly susceptible to cyber attacks. Intrusion detections at PT ABC reached 79,575 in 2021, and malware, botnets, targeted attacks, malicious websites/domains, and ransomware attacks may cause considerable financial losses. The implication of these incidents is that employees' awareness of information security is critical, in addition to security technologies like firewalls and monitoring tools. To enhance employees' knowledge of information security, this study aims to evaluate the information security awareness among PT ABC personnel using the HAIS-Q survey instrument alongside ISO/IEC 27001:2013 criteria. The study will provide valuable recommendations to improve the organization's security protocols. This research intends to investigate the correlation between employees' knowledge, attitude, and behavior towards information security. Data was collected through a questionnaire and analyzed using the Pearson Correlation, Cronbach's Alpha, descriptive statistics, linear regression, and Kruskal-Wallis test method. The study findings suggest that the overall information security awareness level among employees is "Good". However, certain areas like internet usage, information handling, asset management, incident reporting, and the use of mobile devices need improvement. To address these areas, the study recommends promoting information security awareness according to employee categories.**

Keywords*—Security awareness; data; information; ISO/IEC 27001:2013

I. Introduction

The Indonesian government through Presidential Regulation No. 82 of 2022 [1] pays attention to and is committed to protecting Vital Information Infrastructure due to the abuse of information and electronic transactions. Threats to the security of vital objects such as power plants have been experienced by the Gundremmingen nuclear power plant in Germany in 2016 where the "W32.Ramnit" and "Conficker" viruses were attacked through an employee's USB device[1].

The 2021 BSSN Report on Cybersecurity Monitoring reports that one of the background causes of data leaks is phishing [2]. The phishing method is where the hacker infiltrates malicious codes through an e-mail or website page during internet browsing [3][4]. Monitoring data from PT ABC states that the number of intrusion detections during 2021 was 79,575. Cyber attacks such as malware, botnets, targeted attacks, malicious websites/domains, and ransomware attacking the company can result in significant financial losses [3][4]. The lesson learned from these incidents is the need for information security awareness among employees at PT ABC, as security technologies such as firewalls or monitoring tools play an important role in security, but the human factor must also be considered [4].

The measurement of awareness of information security has been the subject of numerous prior studies. Vina Effendy et al. (2022) conducted a study utilizing the HAIS-Q modeling to evaluate the level of information security awareness at XYZ polytechnic. The findings of the study revealed that the level of awareness was at a medium level at the research site, indicating the need for further monitoring to enhance the level of awareness. However, the authors did not provide recommendations based on employee criteria [5]. Another study by Aulia Zulfia et al. (2019) employed the HAIS-Q method to measure information security awareness at PT PQS. Nevertheless, the authors did not provide recommendations based on employee criteria [6]. In a similar vein, Rahardi Prakoso et al. (2020) measured awareness of information security among online transportation users using the HAIS-Q method. The authors identified the areas that require improvement, but did not provide recommendations based on sub-area categories among respondent demographics [7].

The Human Aspects of Information Security-Questionnaire (HAIS-Q) is a widely recognized tool for evaluating global information security awareness. Numerous studies, including [5][6][7][8][21], have utilized the HAIS-Q in various contexts, spanning commercial enterprises, academic institutions, and government agencies. Despite its extensive adoption, previous research has yet to integrate the HAIS-Q with the ISO/IEC 27001:2013 standard, and no research has specifically investigated the extent of awareness of information security among employees of PT ABC.

The motivation described above has instigated a research initiative aimed at assessing the awareness of information security of the PT ABC personnel. The HAIS-Q survey instrument, in conjunction with the ISO/IEC 27001:2013 criteria will be utilized to achieve this goal. The outcomes of this investigation will furnish recommendations for enhancing the organization's security protocols. It is expected that these

[1]S. Christoph and A. Eric, 'German nuclear plant infected with computer viruses, operator says', *Reuters*, 2016, https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS, (accessed 10 October 2022)

insights will have a favorable influence on the information security awareness level at PT ABC.

The ensuing section constitutes the second component of this paper and aims to expound upon the literature review. Subsequently, the third section delineates the theoretical framework, followed by the fourth section which explicates the research methodology. The fifth section comprises a thorough analysis and discourse of the outcomes. Finally, a conclusion will be presented to summarize the findings.

II. Literature Review

A. Information Security Awareness

The field of information security is concerned with safeguarding both information and the systems utilized to transmit, store, or manipulate it [9]. Management of information security entails not only considerations of technology, but also concerns pertaining to human users of the system, as evidenced by the importance of information security awareness [6]. Information security awareness encompasses two distinct dimensions, namely the degree to which users comprehend information security practices and the extent to which they are willing to adhere to organizational policies, rules, and guidelines [5]. The 2021 Annual Cybersecurity Monitoring Report [2] identifies weak human awareness as the primary factor contributing to anomalous network traffic. Cybersecurity training and awareness programs can be broken down into three components [10].

1) Education, which aims to impart wisdom on the importance of information security for the organization.

2) Training, which teaches users how to use security functions in the information system and in their work processes; and

3) Awareness, which builds on the foundation provided by education and training to promote individuals' knowledge of and adherence to best security, safety, and privacy practices [11].

B. HAIS-Q and KAB (Knowledge-Attitude-Behavior) Model

The Human Aspects of Information Security Questionnaire (HAIS-Q) is a validated assessment tool that enables the evaluation of individuals' level of awareness related to information security [12]. The HAIS-Q encompasses seven distinct domains, namely, password management, email usage, internet usage, social media utilization, mobile devices usage, information controlling, and incident reporting [4]. Furthermore, these seven areas are classified into three dimensions that are commonly known as KAB (Knowledge, Attitude, and Behavior) [13]. Each dimension can be elucidated as follows: a) Knowledge pertains to an individual's comprehension of information, b) Attitude denotes an individual's opinion, and c) Behavior pertains to an individual's disposition to undertake actions.

Users with high scores according to HAIS-Q perform better in phishing experiments, showing that HAIS-Q is a good framework for measuring users' information security awareness level [14].

C. ISO/IEC 27001:2013

The ISO/IEC 27001:2013 standards are universally employed for managing information security. These requirements dictate the establishment, implementation, maintenance, and continuous improvement of an organization's strategic decisions [15]. Moreover, they govern the application of management systems based on the PDCA approach, along with supplementary information security controls.

ISO/IEC 27001:2013 consists of 7 clauses and 14 information security control areas comprising 114 control points. Like other ISO standards based on high level PDCA this information security management system standard has a difference in clause 8, which is operation. The main point of attention is how to control information security risks outlined in Annex A.

This research focuses on some information security controls found in Annex A, within the scope of individuals' awareness of information security. Out of the 114 existing controls, some relevant to individual awareness will be selected, such as mobile devices (A.6.2.1), password management (A.9.4.3), email usage (A.13.2.3), internet usage (A.13.2.1), social media usage (A.18.1.4), information handling (A.8.3), incident reporting (A.16.1.3), and asset management (A.12.3 and A.12.5).

D. Validation and Reliability Test Method

1) Validation test: The method used to identify the validity of the questionnaire data is the Pearson Method [16]. Bivariate Pearson Correlation is used to determine the correlation between two variables x and y based on Eq. (1).

$$r = \frac{\left(\sum xy - \frac{\sum x \sum y}{N}\right)}{\sqrt{\left(\sum x^2 - \frac{(\sum x)^2}{N}\right)\left(\sum y^2 - \frac{(\sum y)^2}{N}\right)}}, \quad -1 \le r \le +1 \qquad [16] \ (1)$$

The variables in the formula are defined as follows: r is the Bivariate Pearson Correlation coefficient, N represents the number of data points, while x and y represent the first and second variables, respectively.

2) Reliability test: In identifying the reliability value of the questionnaire data, this research uses the Cronbach's Alpha method [16]. The Cronbach's Alpha value is used to measure internal consistency based on Eq. (2).

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum {s_i}^2}{{s_t}^2}\right) \qquad [16] \ (2)$$

where k is the number of questions, s_i is the variance of each question item, s_t is the variance of the group, and α is the reliability value.

3) Linear regression: In the realm of hypothesis testing for the K-A-B relationship, the Linear Regression approach (as detailed in research [16]) is utilized to ascertain the degree to which the independent variable x can affect variations in the dependent variable y. Eq. (3) is employed to perform regression analysis and determine the R-squared value, which indicates the extent to which the independent variable can

account for variability in the dependent variable. The formula for R-squared, denoted as r^2, is presented in study [16] as follows.

$$r^2 = \frac{\left(\sum xy - \frac{\sum x \sum y}{N}\right)^2 / \left(\sum x^2 - \frac{(\sum x)^2}{N}\right)}{\left(\sum y^2 - \frac{(\sum y)^2}{N}\right)} \quad [16] (3)$$

In Eq. (3), *N* refers to the number of data points, *x* denotes the first variable, and *y* represents the second variable.

4) Descriptive statistics: The Mean value is used to determine the average value of a variable based on Eq. (4).

$$\bar{x} = \frac{\sum x}{N} \quad [16] (4)$$

where $\bar{x}$ is the mean, *N* is the number of data, and *x* is the value of the variable.

The computation of the degree of variability in a variable is ascertained by the employment of the Standard Deviation (SD) value in accordance with Eq. (5), which is represented as:

$$\sigma = \sqrt{\frac{\sum x^2 - \frac{(\sum x)^2}{N}}{N}} \quad [16] (5)$$

In this formula, σ refers to the standard deviation value, *x* represents the value of the variable, *N* signifies the total number of data [16].

E. Significant Difference Test

The Kruskal-Wallis Test [16] is employed in statistical analysis to assess the degree of variation between two or more groups, pertaining to a particular area of interest, by examining values that signify significant differences. As a non-parametric, rank-based test, this method utilizes the mean rank to determine the extent of variation between groups.

The mean rank value is calculated based on Eq. (6):

$$\overline{R_A} = \frac{\sum_{i=1}^{n_A} R_{Ai}}{n_A} \quad [16] (6)$$

where n_A is the number of samples in a particular group for a focus area, R_{A_i} is the rank of a focus area for a sample in a specific respondent group, $\overline{R_A}$ is the mean rank of a focus area for a single respondent group, *N* is the number of data.

The Kruskal-Wallis Test for a single respondent group is calculated using Eq. (7):

$$H = \frac{n_A[\sum_{i=1}^{n_A}(R_{A_i} - (N+1)/2)^2]}{N(N+1)/12} \quad [16] (7)$$

III. THEORETICAL FRAMEWORK

The theoretical frameworks used in this research are the KAB Dimensions, HAIS-Q, and ISO/IEC 27001:2013. To measure the level of awareness of information security, it is required to measure the levels of Knowledge, Attitude, and Behavior from the employees' perspective, this is based on the theory proposed by Schrader & Lawless (2004) [13]. The researcher then focuses the measurement area on some measurement items based on HAIS-Q and ISO/IEC 270001:2013. The theoretical framework is shown in Fig. 1.

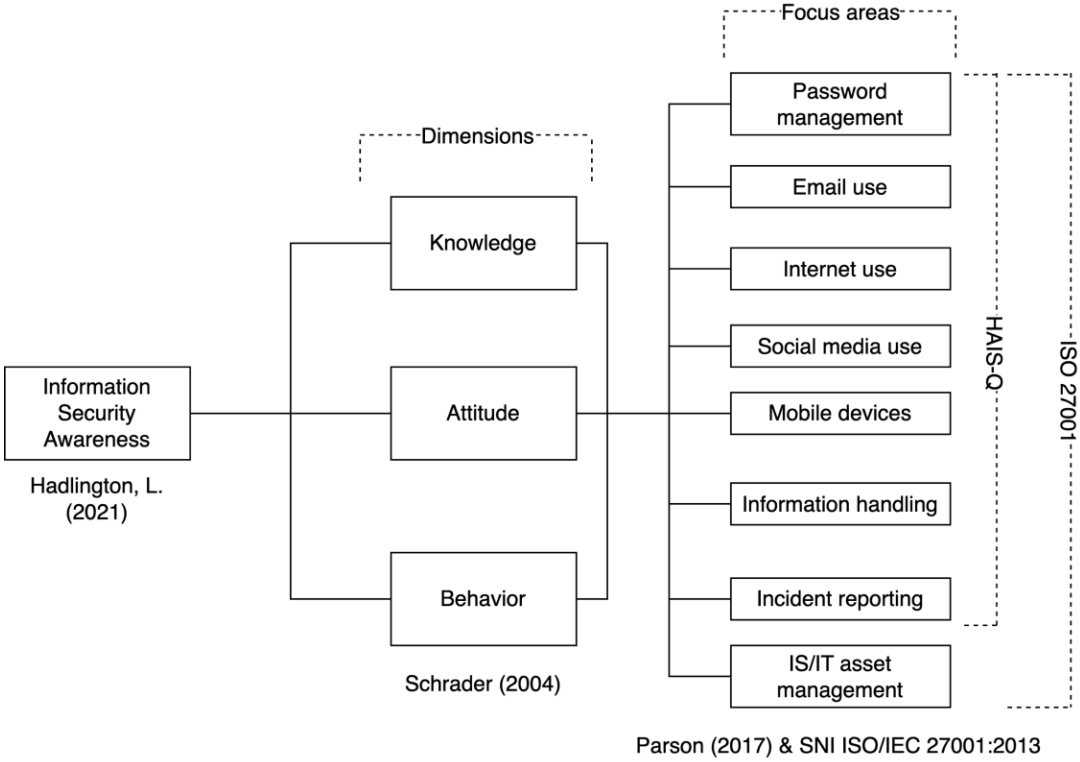

Fig. 1. Theoretical framework.

The research hypothesis consists of:

- H1: The knowledge dimension has a significant effect on the attitude dimension,
- H2: The knowledge dimension has a significant effect on the behavior dimension,
- H3: The attitude dimension has a noteworthy impact on the behavior dimension.

The visual representation of the proposed research hypothesis is depicted in Fig. 2.

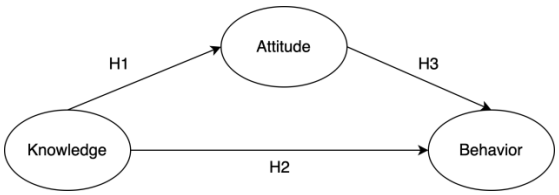

Fig. 2. The research hypothesis.

IV. Research Methodology

This section explains four important things for collecting evidence that justifies the conclusion made, which are A) research instrument, B) stages of research, C) data collection method, and D) data processing and analysis method.

A. Research Instrument

This study utilizes a questionnaire as a research tool, incorporating insights from prior research works, including [5][6][7][8]. The questionnaire is comprised of question components from seven key areas of the HAIS-Q [12] and eight areas of the ISO/IEC 27001:2013 standard [15]. Notably, seven of these areas exhibit significant overlap, encompassing password management, email usage, internet usage, social media usage, mobile device usage, information controlling, and incident reporting. However, one area - pertaining to IT/IS asset management - does not share this overlap. Consequently, the focus areas for this study encompass password management, email usage, internet usage, social media usage, mobile device usage, information controlling, incident reporting, and IT/IS asset management. Additionally, each of these focus areas is further segmented into three distinct dimensions, namely Knowledge, Attitude, and Behavior (K, A, B), as outlined in Table I.

The research tool employed in this study comprises a comprehensive questionnaire consisting of 48 items that are designed to assess the levels of information security awareness among the respondents. The questionnaire is conducted to evaluate the knowledge, attitude, and behavior of the participants, pertaining to eight key areas of focus. Answers are given using the Likert scale 1-5 (1: Strongly Disagree, 2: Disagree, 3: Neutral, 4: Agree, 5: Strongly Agree).

B. Stages of Research

The stages of research of this study can be outlined as follows:

1) Research problem identification: Identify the research problem, which is the need to measure employee information security awareness in PT ABC.

2) Literature review: Conduct a comprehensive review of relevant literature on information security awareness, employee behavior, and security culture in the power generation sector.

3) Research design: Determine the research design, including the research approach, data collection methods, sample size, and data analysis techniques.

4) Data collection: Collect data from the employees using survey questionnaires.

5) Data processing and analysis: Analyze the data using the Pearson Correlation, Cronbach's Alpha, descriptive statistics, linear regression, and Kruskal-Wallis test method.

6) Results interpretation: Interpret the results and draw conclusions based on the findings, highlighting the level of employee information security awareness in PT ABC.

7) Discussion: Discuss the implications of the findings for PT ABC's information security management system and suggest recommendations for improving employee information security awareness.

8) Conclusion: Summarize the main findings and conclusions of the study, and highlight its contributions to the field of information security awareness in the power generation sector.

TABLE I. Focus Area of Information Security Awareness

Focus Area	Sub-Area	Focus Area Code	Indicator Code (K, A, B)
Password management	Sharing password	MP	KMP, AMP, BPM
	Safe password usage		
Email use	Clicking on a link in an email from an unknown sender	EM	KEM, AEM, BEM
	Opening an email attachment from an unknown sender		
Internet use	Downloading a file	IN	KIN, AIN, BIN
	Entering information into the internet		
Social media use	Social media privacy settings	MS	KMS, AMS, BMS
	Posting about work		
Mobile devices	Sending sensitive information over Wi-Fi	PM	KPM, APM, BPM
	Hacking technique: shoulder surfing (observation)		
Information handling	Disposal of sensitive document printouts	PF	KPF, APF, BPF
	Use of USB/other removable media		
Incident reporting	Reporting suspicious behavior	PD	KPD, APD, BPD
	Reporting all incidents		
IS/IT asset management	Regulations regarding the installation of software on agency-owned IT assets	MA	KMA, AMA, BMA
	Data backup		

C. Data Collection

The current research utilized a questionnaire comprising 48 items, distributed via Google Form and administered to 150 employees of PT ABC using a sampling strategy. The questionnaire consisted of eight focus areas, each of which contained two questions pertaining to the dimensions of Knowledge, Attitude, and Behavior. The final sample size consisted of 130 participants, from whom the research team successfully obtained data.

D. Data Processing and Analysis Method

The method for testing validity is using Bivariate Pearson Analysis (Pearson Product Moment Correlation). The Pearson value for all variables is greater than the critical value of 0.172 based on the Pearson Critical Value Table with a sample size of 130 and a significance value of 0.05 2-tailed.

The reliability test was done using Cronbach Alpha, to test the reliability of the measurement indicators used in the research. According to J. Hair (2017), a Cronbach's Alpha value above 0.7 is considered reliable [17].

Linear regression is used to test the hypothesis with the help of SPSS software. The output from SPSS is then processed using Microsoft Excel for descriptive statistical analysis that produces mean and standard deviation data for each sub-area in the knowledge, attitude, and behavior dimensions. The index value is obtained by dividing the total score by the maximum Likert scale value (Y) multiplied by 100% as in Equation (8).

$$Indeks = \frac{Total\ Skor}{Y} \times 100\% \qquad [18]\ (8)$$

The subsequent course of action involves the computation of mean values for each dimension, based on the gathered index values. This leads to the assessment of level of information security awareness. Kruger and Kearney (2006) [18] have classified information security awareness levels into three tiers: Good (80 – 100%), Moderate (60 – 79.99%), and Poor (≤ 59.99%), as illustrated in Table II.

TABLE II. INFORMATION SECURITY AWARENESS CLASSIFICATION [18]

Awareness	Value (%)
Good	80 – 100
Average	60 – 79.99
Poor	≤ 59.99

The Kruskal-Wallis test is a statistical tool commonly utilized to ascertain the significance of categorical variables. Specifically, it is employed to evaluate and compare two or more groups within a particular domain, through the calculation of a significant difference value. This test is a non-parametric procedure, relying on the ranking of the observations (i.e., mean rank) [13].

V. RESULT AND DISCUSSION

A. Demographic of Respondents

The questionnaire was collected from 130 respondents. The demographics of the respondents in this research included job field, job title, education, and length of work at PT ABC. The composition of the respondents can be seen in Table III.

TABLE III. RESPONDENT DEMOGRAPHY

Categories		Total	Percentage
Field	Operation	49	38%
	Maintenance	25	19%
	Engineering	26	20%
	Administration	21	16%
	Other	9	7%
Job title	Structural	33	25%
	Functional	97	75%
Education	S2 (Master)	3	2%
	D4/S1 (Bachelor)	80	62%
	D3 (Three-year diploma)	18	14%
	SMA (High school)	29	22%
Job tenure	≤ 5 years	57	44%
	6 – 10 years	20	15%
	11 – 15 years	24	18%
	≤ 16 years	29	22%

In terms of job field, 38% are in the operations field followed by engineering, maintenance, and lastly, 16% are in administration, while 7% are in other fields. For job title, 75% are functional while the rest are structural. The most common education level among the respondents is D4/S1 with 62%. For length of work, the majority of the respondents have experienced for less than 5 years, accounting for 44%.

B. Validity and Reliability Test

The present study has conducted validity and reliability tests on the variables of interest. The outcome of these tests has been included in the appendix. Specifically, the Pearson correlation coefficient for the APD2 indicator code was found to be 0.108, which falls below the critical value of Pearson. Therefore, the APD2 variable has been excluded from further analysis. On the other hand, Table XV in the appendix presents evidence of the validity of all indicators related to the research variables. Subsequently, a reliability test was conducted, and the results have been presented in Table IV.

This study obtained a Cronbach's Alpha value of 0.919, indicating a high level of internal consistency reliability among the variables assessed. Based on the results of the validity and reliability tests, it can be inferred that the measurement variables utilized in this study exhibit strong validity and reliability.

C. Hypothesis Testing Results

The hypothesis testing was conducted using linear regression method which tests the significance between dimensions in the KAB modeling, which are the Knowledge dimension towards Attitude, the Knowledge dimension towards Behavior and the Attitude dimension towards Behavior.

1) Knowledge – Attitude: The regression coefficient value for the dimension of Knowledge towards Attitude shown in Table VI confirms the significance between the two dimensions (Sig: 0.000).

The findings presented in Table V and Table VI indicate a notable influence of the Knowledge dimension on the Attitude

dimension. The analysis reveals a strong positive correlation (β = 0.803) and a significant level of statistical significance (sig < 0.001) between the two dimensions, with a coefficient of determination (*R-squared*) of 0.644. The empirical relationship between the Knowledge and Attitude dimensions can be expressed by the equation $y = 8.492 + 0.849x$, where y represents Attitude and x denotes Knowledge.

TABLE IV. RELIABILITY TEST RESULT

Cronbach's Alpha	N of Items
0.919	48

TABLE V. COEFFICIENT OF DETERMINATION K-A

Model Summary				
Model	R	R-squared	Adjusted R- squared	Std. Error of the Estimate
1	0.803	0.644	0.642	4.596
Predictors: (Constant), K				

TABLE VI. REGRESSION COEFFICIENTS K-A

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	8.492	3.747		2.266	0.025
K	0.849	0.056	0.803	15.230	0.000

Based on these results, it can be concluded that Hypothesis 1 is supported, as the Knowledge dimension has a significant impact on the Attitude dimension.

2) Knowledge – Behavior: Table VIII shows the regression coefficient values for the dimension of Knowledge towards the dimension of Behavior.

Table VII and Table VIII present the findings of the analysis that demonstrate the Knowledge dimension's impact on the Behavior dimension (correlation β = 0.685, significance sig < 0.001, coefficient of determination *R-squared* = 0.470). The Knowledge-Behavior (K-B) dimensions' relationship can be described by the equation $y = 15.008 + 0.767x$, where y represents the Behavior dimension, and x represents the Knowledge dimension. Thus, the results indicate that an improvement in the Knowledge dimension can lead to a corresponding increase in the Behavior dimension.

Therefore, it can be concluded that Hypothesis 2 can be accepted. The dimension of Knowledge has a significant impact on the dimension of Behavior.

3) Attitude – Behavior: Table X shows the regression coefficient values for the relationship between the Attitude dimension and the Behavior dimension.

The analysis conducted on the data presented in Tables IX and X indicate that Attitude significantly influences Behavior, as evidenced by a strong positive correlation (β = 0.807) and a high level of statistical significance (sig < 0.001), with a coefficient of determination (*R-squared*) value of 0.652. These findings suggest that enhancing employees' attitude towards information security may effectively lead to a positive change in their behavior, which can ultimately lead to better security practices in the organization. The Attitude-Behavior (A-B) relationship can be stated with the equation $y = 10.540 + 0.855x$ where y represents Behavior and x represents Attitude.

Therefore, it can be concluded that Hypothesis 3 can be accepted. The Attitude dimension has a significant impact on the Behavior dimension. The results of the hypothesis test as shown in Fig. 3.

TABLE VII. COEFFICIENT OF DETERMINATION K-B

Model Summary				
Model	R	R-squared	Adjusted R-squared	Std. Error of the Estimate
1	0.685	0.470	0.466	5.943
Predictors: (Constant), K				

TABLE VIII. REGRESSION COEFFICIENTS K-B

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	15.008	4.845		3.098	0.002
K	0.767	0.072	0.685	10.650	0.000

TABLE IX. COEFFICIENT OF DETERMINATION A-B

Model Summary				
Model	R	R-squared	Adjusted R-squared	Std. Error of the Estimate
1	0.807	0.652	0.649	4.816
Predictors: (Constant), A				

TABLE X. REGRESSION COEFFICIENTS A-B

	Unstandardized Coefficients		Standardized Coefficients	t	*Sig.*
	B	Std. Error	Beta		
(Constant)	10.540	3.627		2.906	0.004
A	0.855	0.055	0.807	15.480	0.000

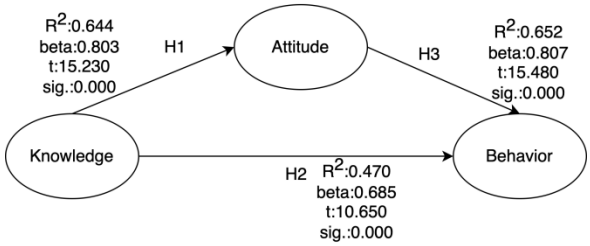

Fig. 3. The results of the hypothesis test.

D. Results of the Information Security Awareness Level Measurement

Table XI presents the findings of the information security awareness level measurement conducted at PT ABC.

The password management, email use, and social media use areas have all met the Good category with regards to the knowledge, attitude, and behavior dimensions. This suggests that employees have a high level of understanding, positive attitude, and appropriate conduct when it comes to password management, email use, and social media use. The results for

the internet use area have been classified under the moderate category, which requires significant attention. As highlighted in the introduction, the internet represents a vulnerable entry point for cyber attacks, including phishing, viruses, and data leakage [8]. Consequently, ensuring that employees exhibit wise and safe internet practices is essential to safeguard the company's information security. Given the moderate category classification, it is imperative for PT ABC to implement measures to improve information security awareness and enhance employee knowledge and behavior in this area.

The mobile device usage area has attained the good category concerning the knowledge and attitude aspects. However, with regards to the behavioral aspect, it is still classified in the moderate category.

In relation to information handling area and incident reporting, both knowledge and behavioral dimensions have achieved the good category; however, in terms of the attitude dimension, it is categorized as moderate.

The assessment of asset management area reveals that it has achieved the Good category with regards to the attitude and behavioral dimensions. However, in terms of knowledge, it has only reached the Moderate category, indicating a need for further improvement.

TABLE XI. RESULTS OF THE INFORMATION SECURITY AWARENESS LEVEL MEASUREMENT

Area/Dimension	*Knowledge*	*Attitude*	*Behavior*
Password management	89.54	83.15	88.92
Email use	83.54	85.69	81.46
Internet use	70.54	75.62	76.00
Social media use	87.23	85.00	81.08
Mobile devices	83.23	82.23	79.92
Information handling	89.62	79.62	87.69
Incident Reporting	85.15	75.31	83.54
IS/IT asset management	79.77	85.69	84.46

Indicators with moderate measurement results can be a priority improvement area that can be enhanced by the company.

1) Behavior dimension based on job tenure category: Table XII shows a significant difference in behavior levels based on the job tenure category in the focus area of email usage, where employees with working experiences of less than five years (mean rank 73.07) have a high value of behavior compared to employees with job tenure 6 to 10 years (mean rank 49.43). Within the information handling focus area, the highest value is in employees with more than 15 years of job tenure (mean rank 77.04) and the lowest is in employees with length of employment 5 to 10 years (mean rank 53.48). Within the incident reporting focus area, the highest value is in employees with more than 15 years of job tenure (mean rank 86.88; mean rank 82.43) and the lowest is in employees with job tenure of less than 10 years (mean rank 58.06; mean rank 58.70).

2) Behavior Dimension based on education level: Table XIII shows a significant difference in the habit of using social media; the lowest is in employees with a Master's degree background and the highest is in employees with a High School education background. The highest incident reporting habit is in employees with a SMA (High School) education background and the lowest is in employees with a Master's degree background.

TABLE XII. BEHAVIOR BASED ON JOB TENURE

Indicator		≤ 5 yr *(mean rank)*	6 – 10 yr *(mean rank)*	11 – 15 yr *(mean rank)*	> 15 yr *(mean rank)*	*Sig**
Password management	MP1	64.31	59.53	69.90	68.33	0.733
	MP2	65.12	59.38	65.75	70.26	0.691
Email use	EM1	73.07	49.43	60.96	65.47	0.052
	EM2	63.58	59.98	64.58	73.84	0.528
Internet use	IN1	62.00	60.15	66.25	75.45	0.372
	IN2	66.64	54.48	57.58	77.41	0.075
Social media use	MS1	62.39	69.08	54.21	78.48	0.083
	MS2	68.34	51.33	61.33	73.14	0.119
Mobile devices	PM1	59.61	64.58	69.19	74.66	0.297
	PM2	60.62	64.15	65.35	76.14	0.286
Information handling	PF1	61.28	53.48	70.88	77.64	0.041
	PF2	66.93	49.80	63.83	74.90	0.087
Incident reporting	PD1	58.06	59.60	62.25	86.88	0.003
	PD2	61.06	58.70	61.25	82.43	0.028
IS/IT assets management	MA1	60.66	58.05	68.00	78.09	0.084
	MA2	68.38	50.50	58.94	75.62	0.067

**Kruskal-Wallis test*

TABLE XIII. BEHAVIOR BASED ON EDUCATION LEVEL

Indicator		SMA *(mean rank)*	D3 *(mean rank)*	D4/S1 *(mean rank)*	S2 *(mean rank)*	*Sig**
Password management	MP1	68.48	60.78	65.03	77.50	0.812
	MP2	65.95	80.56	62.69	45.83	0.109
Email use	EM1	56.12	71.28	67.84	59.00	0.360
	EM2	62.40	76.00	64.45	60.50	0.597
Internet use	IN1	63.02	74.67	65.18	43.00	0.489
	IN2	73.17	69.25	62.68	44.00	0.337
Social media use	MS1	76.17	76.08	60.47	33.00	0.046
	MS2	66.97	76.42	61.44	94.00	0.151
Mobile devices	PM1	72.16	73.78	61.67	53.67	0.362
	PM2	62.34	71.86	64.94	72.67	0.809
Information handling	PF1	73.64	70.75	61.12	72.17	0.284
	PF2	61.03	77.14	64.70	60.17	0.441
Incident reporting	PD1	83.69	71.08	58.03	55.50	0.007
	PD2	77.24	74.86	59.06	67.67	0.057
IS/IT assets management	MA1	64.41	77.81	62.84	73.17	0.356
	MA2	76.09	69.42	60.96	60.67	0.243

**Kruskal-Wallis test*

TABLE XIV. BEHAVIOR BASED ON JOB POSITION

Indicator		Structural *(mean rank)*	Functional *(mean rank)*	*Sig**
Password management	MP1	65.67	65.00	0.922
	MP2	64.04	69.79	0.360
Email use	EM1	67.41	59.88	0.272
	EM2	64.97	67.06	0.773
Internet use	IN1	62.62	73.95	0.123
	IN2	63.60	71.08	0.280
Social media use	MS1	63.78	70.55	0.354
	MS2	65.50	65.50	1.000
Mobile devices	PM1	63.27	72.06	0.224
	PM2	62.16	75.30	0.064
Information handling	PF1	63.46	71.48	0.225
	PF2	64.03	69.82	0.401
Incident reporting	PD1	61.84	76.26	0.041
	PD2	62.40	74.61	0.078
IS/IT assets management	MA1	63.62	71.03	0.264
	MA2	68.12	57.80	0.149

**Kruskal-Wallis test*

3) Behavior dimension based on job postion category: Table XIV shows the behavior level based on job categories. The focus area with a significant difference value less than 0.05 is the incident reporting focus area. In the incident reporting focus area, the highest habit value is in functional employees (mean rank 76.26) and the lowest is in structural employees (mean rank 61.84).

E. Implications

Based on the research results, the following are the practical and theoretical implications:

1) Practical implication: The measurement of information security awareness at PT ABC is presented in Table XI. The results indicate that certain focus areas do not meet the Good category, which suggests that PT ABC should take necessary measures, such as training or actions, to enhance information security awareness. This can serve as a guide for the company to identify the specific areas that require improvement and facilitate the implementation of targeted interventions. Utilizing training programs can be an effective method for improving knowledge and awareness of potential security threats and risks [19]. The focus areas and dimensions that need to be improved are:

- Internet use

It is recommended that PT ABC offer training, socialization, and seminars to employees as a means of enhancing their knowledge and awareness of information security. Additionally, it is advised that the company establish regulations, actions, and punishments against employees who engage in behavior or activities that threaten the security of the company's information system within the internet use focus area. What is included in the internet use focus area such as downloading files carelessly to office devices, accessing suspicious online sites, and entering information into online sites to assist work.

- Mobile devices

PT ABC is authorized to issue warnings, prescribe regulations, and take appropriate actions against employees whose practices may put the company's information system security at risk within the software device use focus area. What is included in the mobile device use focus area such as physical security of devices such as leaving laptops/mobile phones carelessly, sending sensitive information via online networks, and opening sensitive documents near strangers.

- Information handling

PT ABC has the authority to provide notifications, implement regulations, and execute appropriate measures towards employees whose conduct may jeopardize the security of the organization's information system within the information handling focus area. What is included in the information handling focus area such as putting/throwing sensitive documents carelessly, and inserting USB/removable media into office PC/laptops carelessly.

- Incident reporting

PT ABC has the authority to issue warnings, set rules, and take appropriate actions against employees who exhibit behaviors that pose a threat to the security of the company's information system within the incident reporting focus area. What is included in the incident reporting focus area such as reporting suspicious behavior in the office, reporting if there is a dangerous action from a colleague related to the information system security, reporting all incidents/events related to the information system security.

- IS/IT Assets Management

PT ABC can provide training/socialization/seminars to employees to improve their knowledge of asset management such as carelessly installing software, especially pirated software and related data backups.

Table XII - XIV shows the results of the measurement of the dimension of the habits based on the categories of work experience, education, and job type. This categorization can provide insight to the company to identify the strengths and weaknesses of awareness of information security and also facilitate the development of a customized information security training program for employees [20].

Based on the table, PT ABC can provide rules/actions in the more focused areas of information security system based on categories.

If based on work experience category, it is as follows:

- Within the focus area of email use, employees who have worked for over 5 years demonstrate inadequate knowledge of information security systems. Therefore, there is a pressing need to prioritize information security awareness-raising efforts in the email use sector for this category of employees.

- Within the focus area of information handling, employees who have served for 6-10 years exhibit reduced knowledge of information security systems. Consequently, there is a necessity to prioritize awareness-raising efforts on information security within the information handling sector for this group of employees.
- In the incident reporting focus area, employees who have worked for less than 11 years have a lower awareness of information security systems. Consequently, there is a need to focus more on enhancing information security awareness within the incident reporting sector.

Based on education, the focus of increasing awareness of information security can be more focused on the use of social media and incident reporting areas. The details are as follows:

- In the focus area of social media use, employees with S2 education have a lower awareness of information security systems; hence, it is imperative to give more consideration to the awareness of information security within the social media usage domain.
- In the incident reporting focus area, employees with D4/S1 and S2 education have a lower awareness of information security systems, therefore the incident reporting sector requires greater emphasis on information security awareness.

Then, based on job type, PT ABC can focus more on incident reporting on structural employees.

2) Theoretical implications

- In this research, it can be concluded that knowledge has a significant impact on attitudes and habits. Furthermore, the attitude dimension also has a significant effect on behavior.
- Measurement based on respondent category can be done to categorize participants in training/seminar/ awareness-raising activities on information security.

VI. Conclusion

Based on research results, the overall average level of information security awareness among employees at PT ABC is considered good. The findings also highlight specific areas that require improvement to increase awareness about information security, such as internet usage, information handling, asset management, incident reporting, and the use of mobile devices.

The research also showed that the dimension of knowledge influences attitude and behavior, so the information security awareness improvement program can focus on increasing the dimension of knowledge, such as socialization, seminars, and training, as well as punishment systems or monitoring if it focuses on the attitude dimension.

References

[1] "Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV)," 2022.

[2] BSSN, "Laporan Tahunan Monitoring Keamanan Siber 2021," 2021.

[3] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040089.

[4] I. Ghafir et al., "Security threats to critical infrastructure: the human factor," Journal of Supercomputing, vol. 74, no. 10, pp. 4986–5002, Oct. 2018, doi: 10.1007/s11227-018-2337-2.

[5] V. A. Effendy, Y. Ruldeviyani, M. M. Rifa'i, V. A. Rahmatika, W. Nur'aini, and Y. P. Sagala, "Measurement of Employee Information Security Awareness on Data Security: A Case Study at XYZ Polytechnic," in 2022 1st International Conference on Information System and Information Technology, ICISIT 2022, 2022, pp. 272–276. doi: 10.1109/ICISIT54091.2022.9873077.

[6] 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; Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS," 2019.

[7] R. Prakoso, Y. Ruldeviyani, K. F. Arisya, and A. L. Fadhilah, "Measurement of Information Security Awareness Level: A Case Study of Online Transportation Users," in 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020, Dec. 2020, pp. 170–175. doi: 10.1109/ISRITI51436.2020.9315375.

[8] E. Kritzinger, A. da Veiga, and W. van Staden, "Measuring organizational information security awareness in South Africa," Information Security Journal, 2022, doi: 10.1080/19393555.2022.2077265.

[9] L. Hadlington, J. Binder, and N. Stanulewicz, "Exploring role of moral disengagement and counterproductive work behaviours in information security awareness.," Comput Human Behav, vol. 114, Jan. 2021, doi: 10.1016/j.chb.2020.106557.

[10] Nurbojatmiko, A. Fajar Firmansyah, Q. Aini, A. Saehudin, and S. Amsariah, "Information Security Awareness of Students on Academic Information System Using Kruger Approach," in 2020 8th International Conference on Cyber and IT Service Management, CITSM 2020, Oct. 2020. doi: 10.1109/CITSM50537.2020.9268795.

[11] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of Information Security Awareness among Palestinian Learners," in 2021 International Conference on Information Technology, ICIT 2021 - Proceedings, Jul. 2021, pp. 21–26. doi: 10.1109/ICIT52682.2021.9491639.

[12] 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.

[13] P. G. Schrader and K. A. Lawless, "The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments," Performance Improvement, vol. 43, no. 9, pp. 8–15, Sep. 2004, doi: 10.1002/pfi.4140430905.

[14] D. Fujs, S. Vrhovec, and D. Vavpotic, "Know Your Enemy: User Segmentation Based on Human Aspects of Information Security," IEEE Access, vol. 9, pp. 157306–157315, 2021, doi: 10.1109/ACCESS.2021.3130013.

[15] "SNI ISO/IEC 27001:2013 Standar Nasional Indonesia Badan Standardisasi Nasional," 2016. [Online]. Available: www.bsn.go.id.

[16] S. Dowdy, S. Weardon, and D. Chilko, Statistics for Research, Third. Hoboken, New Jersey, USA: John Wiley & Sons, Inc., 2004.

[17] J. F. Hair, G. T. M. Hult, C. M. Ringle, and Marko. Sarstedt, A primer on partial least squares structural equation modeling (PLS-SEM). 2007.

[18] 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.

[19] 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.

[20] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness,"

Comput Human Behav, vol. 69, pp. 151–156, Apr. 2017, doi: 10.1016/j.chb.2016.11.065.

[21] Al-Shanfari I, Warusia Yassin, Nasser Tabook, Roesnita Ismail, Anuar Ismail, "Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 8, 2022.

APPENDIX

TABLE XV. INSTRUMENT VALIDITY TEST RESULTS

Indikator	Pearson Correlation	Sig. (2-tailed)	N	Indikator	Pearson Correlation	Sig. (2-tailed)	N
KMP1	0.374	0.000	130	APM1	0.555	0.000	130
KMP2	0.402	0.000	130	APM2	0.631	0.000	130
KEM1	0.285	0.001	130	APF1	0.234	0.007	130
KEM2	0.290	0.001	130	APF2	0.550	0.000	130
KIN1	0.552	0.000	130	APD1	0.512	0.000	130
KIN2	0.562	0.000	130	APD2	0.108	0.220	130
KMS1	0.456	0.000	130	AMA1	0.590	0.000	130
KMS2	0.390	0.000	130	AMA2	0.398	0.000	130
KPM1	0.416	0.000	130	BMP01	0.506	0.000	130
KPM2	0.486	0.000	130	BMP02	0.615	0.000	130
KPF1	0.370	0.000	130	BEM1	0.447	0.000	130
KPF2	0.521	0.000	130	BEM2	0.437	0.000	130
KPD1	0.318	0.000	130	BIN1	0.627	0.000	130
KPD2	0.492	0.000	130	BIN2	0.513	0.000	130
KMA1	0.563	0.000	130	BMS1	0.382	0.000	130
KMA2	0.213	0.015	130	BMS2	0.359	0.000	130
AMP1	0.491	0.000	130	BPM1	0.539	0.000	130
AMP2	0.461	0.000	130	BPM2	0.399	0.000	130
AEM1	0.539	0.000	130	BPF1	0.599	0.000	130
AEM2	0.565	0.000	130	BPF2	0.549	0.000	130
AIN1	0.568	0.000	130	BPD1	0.583	0.000	130
AIN2	0.596	0.000	130	BPD2	0.591	0.000	130
AMS1	0.467	0.000	130	BMA1	0.619	0.000	130
AMS2	0.514	0.000	130	BMA2	0.397	0.000	130