Accredited SINTA 2 Ranking
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online at: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 9 No. 2 (2025) 364 - 373 e-ISSN: 2580-0760

Strategic Approach to Enhance Information Security Awareness at ABC Agency

Fandy Husaenul Hakim[1*], Muhammad Hafizhuddin Hilman[2], Setiadi Yazid[3]
[1,2,3] Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia
[1]fandy.husaenul@ui.ac.id, [2]muhammad.hilman@ui.ac.id, [3]setiadi@cs.ui.ac.id

Abstract

Information security awareness (ISA) is crucial to an organization's cybersecurity strategy, particularly since employees are often the last defense against cyberattacks. Despite regular communication on cybersecurity threats, the ABC Agency has not evaluated the level of ISA among its employees, leaving a gap in understanding the effectiveness of its awareness programs. This is critical, as the agency handles highly confidential data that could be at risk of accidental or intentional leaks. The Kruger Approach and the Human Aspect of Information Security Questionnaire (HAIS-Q) were used in this study to measure the ISA levels of employees at the ABC Agency. We employed the Analytic Hierarchy Process (AHP) method to analyze data collected from 86 respondents. The findings indicate that ABC Agency employees demonstrate satisfactory ISA overall. However, the "Internet Use" dimension received a medium rating, underscoring the necessity for focused enhancements in this domain. These results underscore the importance of tailoring information security awareness programs to address specific weaknesses. We provide strategic recommendations to enhance the agency's cybersecurity posture. Furthermore, this study opens avenues for future research on ISA measurement across various public and private organizations.

Keywords: *information security awareness; information security awareness strategies; Kruger approach; Human Aspect of Information Security Questionnaire (HAIS-Q); Analytic Hierarchy Process (AHP)*

How to Cite: F. H. Hakim, M. H. Hilman, and S. Yazid, “Strategic Approach to Enhance Information Security Awareness at ABC Agency”, *J. RESTI (Rekayasa Sist. Teknol. Inf.)* , vol. 9, no. 2, pp. 364 - 373, Apr. 2025.
DOI: https://doi.org/10.29207/resti.v9i2.6218

1. Introduction

Information security awareness (ISA) is an important aspect of maintaining the confidentiality of data held by individuals and organizations [1]. Information security covers data related to work or business operations and sensitive personal data. In the digital age, where cyber threats are constantly evolving and irresponsible parties can exploit security gaps, the protection of personal information is becoming increasingly crucial [2], [3]. Therefore, building awareness of the importance of maintaining information security, both at the individual and organizational level, is a vital step to prevent data leaks and safeguard privacy [4].

ISA is a critical aspect of safeguarding sensitive information in organizations. While organizations have invested heavily in technology to mitigate cyber threats, many studies show that human factors remain the weakest link in information security [4], [5]. Organizations often fail to detect human-caused leaks because such behavior is difficult to predict with conventional security systems [6]. The National Cyber and Crypto Agency reported in 2023 that attackers frequently capitalize on individuals’ lack of vigilance, making human behavior one of the most targeted vulnerabilities [7]. The proliferation of cyberattacks underscores the importance of evaluating the ISA levels within organizations, particularly in institutions like ABC Agency, which manages sensitive data.

The ABC Agency is responsible for conducting inspections and analyses in the financial industry. In carrying out its duties, the ABC Agency stores and manages highly confidential financial data. The organization utilizes this financial data as its primary source of information, processing it and submitting it to the authorities for potential financial crimes. However, despite the organization's reliance on strict security policies and employee training programs, incidents of negligence and non-compliance among employees persist, highlighting gaps in their information security awareness. Interviews with information security SMEs

Received: 07-12-2024 | Accepted: 12-04-2025 | Published Online: 19-04-2025

at ABC Agency reveal that although the agency conducts annual briefings, disseminates security information through screensavers, and circulates official reminders, employees continue to demonstrate behaviors that undermine organizational security efforts [6].

ABC Agency has never measured the level of information security awareness among its employees, despite it being a crucial step in ensuring the effectiveness of information security-related training and socialization programs [5], [8]-[10]. According to Alshaikh et al. [10], the importance of evaluating and measuring information security awareness lies in its ability to ensure employee compliance with security policies and mitigate potential internal risks caused by negligence or non-compliance. Without measurable data, the agency cannot identify which areas of ISA require improvement or design targeted strategies to mitigate these risks. Therefore, measuring the level of information security awareness at ABC Agency is crucial. The CIO of ABC Agency expects the ISA condition to be at a satisfactory compliance level. Through this research, we hope to demonstrate the potential for improving or enhancing employee ISA.

Researchers have developed and tested various frameworks to measure information security awareness—the research conducted by I et al. [1] measures ISA in the public sector by considering five factors: control/prediction, motivation, deterrence, technical-related, and facilitating conditions. This study employs protection motivation theory (PMT), theory of planned behavior (TPB), and general deterrence theory (GDT) to enhance employees' intention for information security awareness. Additionally, technical aspects, such as educational and training programs and facilitating conditions, serve as organizational efforts to assist employees in improving their ISA intentions.

The research by Chumaera et al. [11] utilized the Kruger Approach, a combination of the knowledge-attitude-behavioral (KAB) model, to determine the level of ISA in various areas, each with its own weighting criteria. Research was conducted on high school and undergraduate students. They revealed that the level of students' knowledge affects their attitudes and behaviors related to information security practices. Sari et al. [12] reveal that a high level of knowledge about information security does not necessarily indicate a high level of security awareness. In the study, smartphone users showed an 86% (good) level in the knowledge dimension, but the behavior dimension only reached 73%. (average). These findings indicate that the high number of information security breach incidents experienced by smartphone users is due to their behavior of not paying enough attention to information security. The study by Nurbojatmiko et al. [13] utilized six dimensions for measurement: knowledge, attitude, behavior, confidentiality, integrity, and availability. The study involved students from one of Indonesia's universities. The results show that the students' ISA level averages 75%. Gardenia et al. [14] conducted another study at Aerospace Air Marshal Suryadama University, focusing on aligning with organizational needs by incorporating data security and cyber-attacks. The result is that knowledge, attitude, and behavior positively and significantly influence each other.

Research using the Human Aspect of Information Security Questionnaire (HAIS-Q) method has been widely conducted in both the public and private sectors. Hermawan et al. [15] conducted an ISA-level measurement at XYZ Agency, which operates in the social and labor sectors. The final analysis results show that the level of information security awareness among employees is at a "good" level, with a final score of 80.82%. Ernita et al. [16] conducted an ISA-level measurement at a bank using HAIS-Q, demonstrating that the banking sector's employees had an ISA level of 83.46%, emphasizing the role of continuous education in fostering awareness. Zulfia et al. [17] conducted an ISA-level measurement in the private sector. The research results show that employees have sufficient awareness of information security. However, several aspects of ISA require improvement, particularly in email and internet use.

Researchers can also combine focus areas from the HAIS-Q method with focus areas from other methods to measure the level of ISA (Rosihan et al. [18] measured the level of ISA by adopting the KAMI Index and HAIS-Q instruments. To measure information security, Rosihan added focus areas on information security policy and workstation policy, referencing SNI ISO/IEC 27001 and considering security awareness. However, HAIS-Q does not cover all focus areas, including the lack of adherence to organizational policies and the understanding that actions carry consequences. In this research, the focus areas measured are those in HAIS-Q, adherence to policy, and actions that carry consequences. These aspects are important in encouraging proactive behavior among employees, especially to ensure that they not only understand the rules but also take responsibility for the consequences of their actions [12], [19], [20]. In addition, this research was conducted across all units in the ABC Agency with 86 respondents. Hermawan et al. [15] conducted their research solely at one branch of the XYZ Agency, with 30 respondents. This does not represent the agency's overall ISA level.

Despite these contributions, there remains an exigent need to delve deeper into the specific dimensions of ISA, particularly within the context of public sector organizations that handle confidential information. Public sector entities often handle sensitive data, and their responsibilities can differ significantly from those in the private sector.

This research aims to understand the level of employee awareness about information security and identify areas that require improvement. The Analytic Hierarchy Process (AHP) method, which prioritizes and ranks the relative importance of each dimension within the KAB model based on the data collected from respondents, calculates the level of ISA. This method allows for the quantification of subjective judgments and provides a structured approach to identifying the most critical areas for improvement [15].

An instrument combining the Kruger Approach and HAIS-Q identifies the areas that require improvement. Organizations can use this information to design more effective information security awareness programs catering to employees' needs. Therefore, the research questions in this paper are:

RQ 1: What is the level of employee awareness of information security at ABC Agency, and which focus areas need improvement?

RQ 2: What recommendations can be given to the organization based on the measurement results to ensure ABC Agency achieves a good ISA level?

The scope of this research is conducted at ABC Agency and focuses on measuring employee awareness of information security using AHP and finding which focus areas need to be improved using the Kruger Approach and HAIS-Q.

This research brings ISA measurement to the public sector by focusing on a government agency that handles highly sensitive financial data and giving empirically based recommendations that not only fill in gaps in ISA but also help organizations design targeted strategies to raise employee awareness.

2. Research Methods

This chapter explains the methodology used in this research to achieve the objectives. The discussion covers the research process, instruments, data testing, and data processing methods.

2.1 Research Process

This research aims to assess the level of ISA in the ABC Agency environment and pinpoint areas that require improvement. Several stages are carried out in this research, as shown in Figure 1.

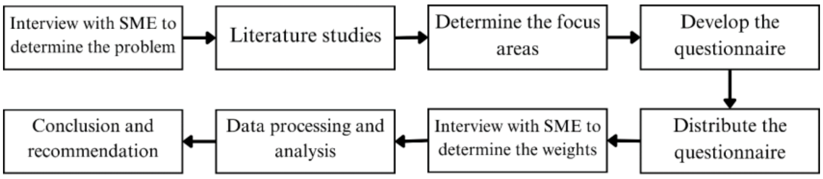
Interview with SME to determine the problem
Literature studies
Determine the focus areas
Develop the questionnaire
Distribute the questionnaire
Interview with SME to determine the weights
Data processing and analysis
Conclusion and recommendation

Figure 1. Research Process

The following is an explanation of the research stages:

Interview with SMEs to determine the problem: The first stage was conducting interviews with subject matter experts (SMEs) to identify and understand the specific problems or challenges within the organization. The gathered information aids in defining the research focus and aligning it with real-world issues.

Literature studies: This stage thoroughly reviews existing literature, research papers, and relevant studies. The goal is to gather insights, theories, and data from previous works to inform the research design and methodology. This helps build a solid foundation for understanding the current research state and identifying gaps.

Determine the focus area: Based on the findings from the literature review and input from SMEs, the focus areas are defined. The research utilized the model dimensions of KAB (knowledge, attitude, behavior), with each dimension elaborated through 9 specific focus areas as outlined by the Kruger Approach and HAIS-Q.

Develop the questionnaire: The questionnaire contained 75 questions about respondents' opinions on information security issues relating to pre-determined focus areas. At this stage, one IT person and one non-IT person conduct a readability test.

Distribute the questionnaire: Using a purposive sampling technique, distribute the completed questionnaire to respondents who were ABC Agency employees.

Interview with SMEs to determine the weights: An interview was conducted to determine the weights for each focus area.

Data processing and analysis: The next stage was to process the questionnaire results. We conduct validity and reliability tests, then analyze and calculate the results using dimension weights and focus area weights to get the results.

Conclusion and recommendations: The final stage is to draw conclusions based on the analyzed data. This includes summarizing key findings, discussing their implications, and providing recommendations for future research or practical applications.

2.2 Research Instrument

We used the questionnaire to evaluate all dimensions and focus areas. The questionnaire is divided into two segments. The first segment was to determine the demographics of the respondents, including gender, age, education level, and work period [15]. The second segment contained 75 questions about ISA related to the KAB model dimensions and 9 predetermined focus areas. Respondents must answer using a Likert scale of 1–5 for each question, where 1 means “strongly disagree” and 5 means “strongly agree” [21].

The research population consisted of permanent employees at ABC Agency. We use the purposive sampling technique, dispersing the population across all departments within the ABC Agency. We use purposive sampling because the target of the sample has a certain characteristic, which is using information technology in daily life and work [22].

2.3 Data Testing Method

To ensure a high level of validity and reliability on questionnaires, we conduct a validity test and a reliability test so the results obtained can be more accurate [23]. We conduct the validity test to assess a measurement instrument's validity (accuracy). The measurement instruments used in this study are questions from a questionnaire. We use the Pearson correlation test to determine the extent of the relationship between the question items and their total value. We then compare the results with the Pearson correlation value in the test table. If the validity value (r) exceeds the significance level of 0.05, the question is considered valid; otherwise, the question is considered invalid.

We conduct the reliability test to determine if the data maintains its consistency and reliability when we repeat the measurement. One of the methods used in the reliability test is the Cronbach's alpha method, which can be seen in Equation 1 [23]:

$$r_{11} = \left[\frac{k}{(k-1)}\right]\left[1 - \frac{\sum \sigma_b^2}{\sigma_t^2}\right] \tag{1}$$

r_{11} is the instrument reliability coefficient (total test), k is the number of valid questions, $\sum \sigma_b^2$ is the total number of item variances, σ_t^2 is the total score variance. We accept calculations using the Cronbach's alpha formula when the r-count exceeds the r-table by 5%. We conducted this study's validity and reliability test using the Statistical Package for the Social Sciences (SPSS) program.

2.4 Data Processing Method

This research employs nine focus areas that combine the focus areas of the Kruger Approach and HAIS-Q, specifically tailored to the organization's needs [19], [24].

The Kruger Approach and HAIS-Q focus areas intersect, allowing us to use this study's focus areas: (1) Password management; (2) Email use, (3) Internet use; (4) Social media use, (5) Mobile device, (6) Information handling, (7) Incident reporting, (8) Adhering to policy; and (9) Actions carry consequences. This research uses AHP to rank and weight various information security dimensions and focus areas [15]. Figure 2 displays the research framework based on the AHP hierarchical structure with goals, dimensions, and focus areas used in this research.

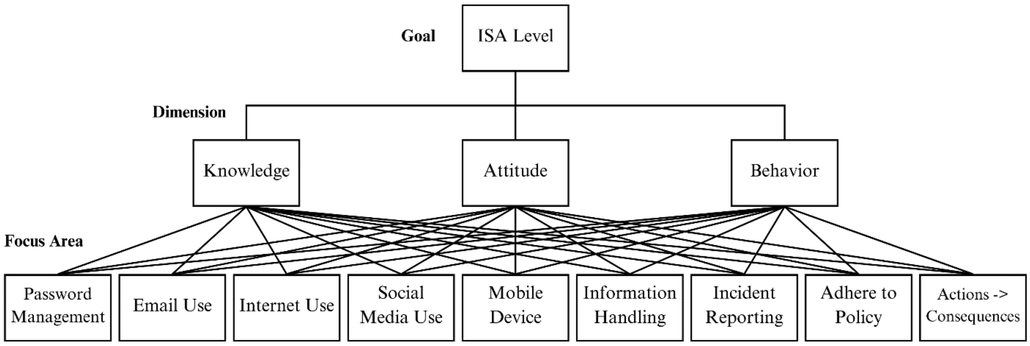

Figure 2. Research Framework Based on AHP

To get the weight of each dimension or focus area requires the opinion of experts. In this research, the weighting of each dimension within the KAB model (criteria) was based on prior research conducted by Kruger and Kearney [19], [20]. Table 1 shows the weighting for each dimension of the KAB model.

Table 1. Weight of Dimensions

Dimensions	Weightings
Knowledge (K)	30
Attitude (A)	20
Behavior (B)	50

Meanwhile, the weighting in each focus area is based on the opinion of the information security SMEs at ABC Agency. The expert is the Chief of the ICT Security Team at ABC Agency, who has experience in Cybersecurity since 2006. The expert creates a pairwise comparison matrix to get the Eigenvector, also known as the local vector, as described in Equation 2 [25].

$$A_w = \begin{bmatrix} 1 & a_{12} & \dots & a_{1n} \\ a_{21} & \dots & a_{ij} & \dots \\ \dots & a_{ji} = 1/a_{ij} & \dots & \dots \\ a_{n1} & \dots & \dots & 1 \end{bmatrix} \tag{2}$$

a_{ij} is the comparison between items i and j.

The eigenvector shows the relative weight of each focus area, which is then used to rank or prioritize the rating on the focus area [15]. Table 2 illustrates the rating of the comparison scores of all focus areas on a scale of 1 to 9, and Table 3 displays the results of the pairwise comparison matrix.

Table 2. Level of ISA

Level	Percentage (%)	Information
Good	80-100	Satisfactory, no action required
Medium	60-79	Monitor, potentially, action is required
Low	0-59	Unsatisfactory, action required

The calculation of focus area weight involves summing the values of each column in the matrix, followed by dividing each column's value by the total of that column to achieve normalization. We then sum and divide the values of each row by the number of elements to determine the weight [15]. Table 4 illustrates the weight of the focus area. According to Table 4, experts at ABC Agency consider information handling, adherence to policy, and password management to be more critical than other focus areas, also shown in Table 5.

Table 3. Comparison Value

Value	Description
1	Equally important compared to the others
3	Slightly more important compared to the others
5	Fairly important compared to the others
7	Very important compared to the others
9	Extremely important compared to the others
2,4,6,8	A value between two adjacent ratings
Reciprocal	If element i is assigned one of the above numbers in comparison to element j, then j will have the reciprocal value when compared to i

Table 4. Pairwise Comparison Matrix of Focus Area

Focus Area	PM	EU	IU	SU	MD	IH	IR	AP	AC
PM	1	8	6	8	5	1	2	1	1
EU	0.125	1	3	7	1	0.125	2	0.143	0.5
IU	0.167	0.333	1	7	0.25	0.125	2	0.143	0.5
SU	0.125	0.143	0.143	1	0.143	0.125	1	0.125	0.25
MD	0.2	1	4	7	1	0.125	7	0.143	5
IH	1	8	8	8	8	1	8	7	8
IR	0.5	0.5	0.5	1	0.143	0.125	1	0.143	0.333
AP	1	7	7	8	7	0.143	7	1	7
AC	1	2	2	4	0.2	0.125	3	0.143	1

Table 5. Weight of Focus Area

Focus Areas	Weightings
Password Management (PM)	17.8
Email Use (EU)	5.3
Internet Use (IU)	4
Social Media Use (SU)	1.7
Mobile Device (MD)	9.6
Information Handling (IH)	32
Incident Reporting (IR)	2.9
Adhere to Policy (AP)	19.9
Actions Carry Consequences (AC)	6.8

After collecting the questionnaires from ABC Agency employees, we measured each focus area's ISA level using the KAB dimensions. Kruger and Kearney [20] developed a method for assessing the level of information security awareness. There are three levels: Green indicates the "good" level, with a score percentage of 80 to 100%. The employee's ISA is satisfactory at this level and does not require further action. The yellow indicates the "medium" level, with a score percentage of 60 to 79%. Monitoring the employee's ISA at this level, with the potential for further action to improve and prevent decline, is necessary. The red indicates the "low" score percentage, ranging from 0 to 59%. At this level, the employee's ISA is unsatisfactory and requires immediate action to prevent a negative impact on the organization.

3. Results and Discussions

We collected 86 respondents. We then analyzed the questionnaire results to determine the ISA level of ABC Agency employees

3.1 Demografic of Respondents

The respondents in this study are permanent employees at ABC Agency who use technology in their daily lives and work. We asked the respondents demographic questions in the first segment of the questionnaire, which included gender, age, education level, and work period. Table 6 displays the demographics of the respondents. The proportion of male and female respondents is nearly equal. Most respondents who answered are young and hold at least a bachelor's degree. In addition, most respondents have also been working for more than 2 years, which means they have been there long enough to understand the rules and work culture at the ABC Agency.

Table 6. Demographics of Respondents

Variable	Item	Total	Percentage (%)
Gender	Male	45	52.3
	Female	41	47.7
Age	21-30	35	40.7
	31-40	42	48.8
	41-50	8	9.3
	> 50	1	1.2
Education Level	Associate	10	11.6
	Bachelor	57	66.3
	Master	19	22.1
Work Period	< 2 years	7	8.1
	2-5 years	38	44.2
	6-10 years	26	30.2
	11-15 years	10	11.6
	> 15 years	5	5.8

3.2 Validity and Reliability Test Results

We conducted validity and reliability tests to ensure the validity and consistency of the collected questionnaires.

Table 7 shows the results of the validity test, revealing that all Pearson values exceed 0.212, the r-table value for 86 respondents at a significance level of 0.05 [23]. These results prove that the collected questionnaire is valid.

Table 7. Validity Test Results

Focus Area	Sub-Area	Knowledge	Attitude	Behavior
PM	Using the same password	0.572	0.713	0.619
	Sharing passwords	0.578	0.591	0.604
	Using a strong password	0.554	0.506	0.510
EU	Clicking on links in emails from known senders	0.638	0.586	0.528
	Clicking on links in emails from unknown senders	0.519	0.583	0.696
	Opening attachments in emails from unknown senders	0.664	0.573	0.465
IU	Downloading files	0.732	0.633	0.812
	Accessing dubious websites	0.453	0.546	0.670
	Entering information online	0.784	0.818	0.534
SU	Social media privacy settings	0.608	0.562	0.562
	Considering consequences	0.664	0.738	0.579
	Posting about work	0.599	0.585	0.516
MD	Physically securing mobile devices	0.580	0.575	0.638
	Sending sensitive information via Wi-Fi	0.696	0.714	0.684
	Shoulder surfing	0.693	0.730	0.737
IH	Disposing of sensitive printouts	0.533	0.638	0.614
	Inserting removable media	0.604	0.618	0.675
	Leaving sensitive material	0.799	0.665	0.687
IR	Reporting suspicious behavior	0.744	0.664	0.803
	Ignoring poor security behavior by colleagues	0.774	0.688	0.739
	Reporting all incidents	0.688	0.533	0.571
AP	The Importance of Information Security Policy	0.819	0.817	0.785
	Adherence to information security policy	0.854	0.795	0.854
AC	Accountability awareness	0.761	0.678	0.710
	Preventive measures	0.781	0.697	0.687

In conducting the reliability test, the author categorized the questionnaire questions into three dimensions: KAB. Cronbach's alpha value for each dimension shows an r-count value above 0.213, which is the r-table value at 5% [23]. This indicates that the questionnaire data is reliable, trustworthy, and consistent. Table 8 presents the results of the reliability test data calculations.

Table 8. Reliability Test Results

Dimension	Cronbach's Alpha
Knowledge	0.874
Attitude	0.889
Behavior	0.892

3.3 Information Security Awareness Measurement Results

To obtain the total awareness value in each focus area, we calculated the average of each KAB variable in each focus area multiplied by the dimension weight specified in Table 1. Meanwhile, to obtain the total awareness value in the KAB dimension, we calculated the average of each KAB variable in each focus area, multiplied by the focus area weight specified in Table 4, resulting in the overall total ISA level.

Table 9 shows that the ISA level of employees at ABC Agency is at the "good" level, with a score of 90.85%. The total scores for each dimension are also at the "good" level, with knowledge scoring 91.14%, attitude scoring 91.02%, and behavior scoring 90.61%. This means that the ISA of ABC Agency employees is satisfactory and does not require further action to significantly improve the ISA level.

Table 9. Results of Information Security Awareness Measurement

Focus Area	K	A	B	Total
Password Management	88.76%	87.36%	90.93%	89.57%
Email Use	85.66%	89.15%	85.81%	86.43%
Internet Use	77.60%	85.74%	78.76%	79.81%
Social Media Use	87.83%	89.07%	86.36%	87.34%
Mobile Device	95.27%	93.10%	94.81%	94.60%
Information Handling	93.41%	92.95%	95.04%	94.13%
Incident Reporting	87.29%	84.96%	88.14%	87.25%
Adhere to Policy	92.33%	93.84%	85.93%	89.43%
Actions → Consequences	92.09%	88.02%	89.53%	90.00%
Total	91.14%	91.02%	90.61%	90.85%

The results of this study align with the research conducted by Gardenia et al. [14], which states that if a person's knowledge level about information security is high, then their attitude and behavior are also likely to be high. This indicates a positive relationship between the three variables. Unlike previous research, such as that conducted by Ernita et al. [16], which only used HAIS-Q and found that the ISA level in the banking sector was at a "good" level (83.46%). In the focus area of "Internet Use," there is a discrepancy between knowledge, attitude, and behavior where the values of knowledge and behavior are low, but the attitude is very high.

The findings of this study indicate that the ISA level of employees at ABC Agency is better than that of other similar organizations that also use AHP in their analysis. Hermawan et al. [15] found that employees in the social and labor sectors had an ISA level of 80.82%. The research conducted by Ernita et al. [16] shows that IT employees at Bank XYZ have an ISA level of 83.46%, and the research conducted by Rosihan et al. [18] shows that employees at the Indonesian Correctional Institution have an ISA level of 85.81%.

3.4 Discussions

Looking at Table 9, we can see that one focus area, Internet Use, still requires improvement, as its overall awareness remains at a “medium” level, with a score of 79.81%. Although the attitude score in the Internet Use focus area is at a “good” level of 85.74%, the knowledge and behavior scores are still at a “medium” level with 77.60% and 78.76%, respectively. The employees are fully aware of the risks associated with downloading files from the internet. However, they continue to do so because these files aid in their task completion. They also know that their computers are equipped with antivirus software and that the office security system is robust enough to prevent virus and malware attacks. "Downloading files" is the sub-area contributing to employees' low knowledge and behavior scores. In this sub-area, the questionnaire question is "I am allowed to download any files to my work computer if the files help me in doing my job" for knowledge and "I download any files to my work computer that will help me complete my job" for behavior. Respondents view “any file” they download as harmless, simply ordinary documents that are not executable, as the office security system will block executable files. Respondents have already chosen wisely which files they can download and cannot. However, employees should resist the temptation to sacrifice security for comfort by downloading any files without considering the potential risks associated with those files [17].

The second-smallest focus area is Email Use, which has a total awareness score of 86.43%. The level of focus in the Email Use area is indeed at a “good” level. However, it wouldn't hurt for the organization to be cautious about this focus area because some employees still consider it normal to click on email links from known contacts. The organization does not directly prohibit employees from clicking links from known contacts. Still, they must be more meticulous about the domain used in the email and whether it matches the organization or not. Consider whether the email's message remains reasonable. It could indicate a hack or a fraudulent email if it deviates by requesting sensitive information like a password. Emails from known contacts could also be forwarded from other parties that could be harmful or phishing emails from spoofed senders [17].

Mobile Device is the focus area with the highest total value, 94.60%. Employees understand the significance of safeguarding their work equipment in public places and refraining from carelessly using public Wi-Fi, particularly when sending work-related files, due to the potential risk posed by Man-in-the-Middle (MitM) attacks [26]. Additionally, employees ensure that others cannot see the monitor screen while performing confidential work.

Information Handling, the focus area considered the most important by experts at ABC Agency, has the second-highest total awareness score with a value of 94.13%. Employees know not to throw confidential documents away or leave them on their desks when they're away. Employees are also aware that carelessly plugging USB flash drives into their devices poses a significant threat to computer systems, as viruses can spread from one computer to another or from one computer to a network [27].

Although the ISA level at ABC Agency is already satisfactory, it is recommended to continue conducting regular and consistent monitoring to maintain that level of ISA [18]. We can implement several strategic recommendations to ensure ABC Agency employees maintain the expected high ISA level. The strategy includes creating a comprehensive security awareness program. The content of the security awareness program must align with the information security policy and be presented through engaging and diverse programs and media [16].

We propose additional recommendations for the existing focus areas. In the focus area of Password Management, the organization already uses Active Directory for password management by implementing a policy of using complex password combinations, including an uppercase letter at the beginning of the password, lowercase letters, numbers, and special characters. However, the National Institute of Standards and Technology (NIST) has updated its password security guidelines and now recommends longer passwords instead of enforcing a combination of at least one uppercase letter, one lowercase letter, numbers, and special characters [28].

In the focus area of Email Use, the organization can provide socialization through phishing email simulation activities sent from senders that appear to be from within the organization's internal network. This aims to train employees to recognize signs of phishing emails, such as suspicious links, requests for sensitive information, or inconsistent sender addresses [29]. Additionally, organizations can enhance their information security culture by posting information on the Intranet or displaying screensavers about cybercrime issues that exploit email media [30].

The focus area of Internet Use can also benefit from implementing the same recommendations. In addition to providing socialization about cyber-attack dangers, organizations can offer regular training on internet risks, such as malware, ransomware, or phishing through websites. Organizations need to provide guideline documents or online modules that explain safe practices in internet usage, including how to evaluate the credibility of websites, identify harmful pop-ups, and choose trustworthy sources for downloading files. We do this to enable employees to identify the warning signs of unsafe websites. Organizations also need to remind employees not to provide personal data over the Internet carelessly [15].

The use of social media is a right for employees to express themselves in the virtual world. However, organizations can warn employees not to indiscriminately share confidential information on social media, whether personal or organizational data. Unknowingly, employees may divulge personal details like birth dates, credit card numbers, contact numbers, or home or office addresses, leaving them vulnerable to exploitation by irresponsible parties. Therefore, organizations must educate their employees on the significance of regularly updating their social media privacy settings and clarifying the permissible and prohibited postings on these platforms [15].

Organizations can implement data encryption and exchange mechanisms using internal cloud technology to help maintain a high level of awareness in the focus areas of Mobile Device and Information Handling. Work-related documents that are confidential should not be stored on laptops, let alone on USB flash drives. Employees can utilize an encrypted internal cloud to exchange data. We do this to prevent data leaks if employees lose their mobile devices due to negligence. Closing access to USB ports and CD/DVD drives is also an effective step to force employees to stop using removable media that are easily lost and contain viruses or malware [27].

Policies and procedures for reporting information security incidents must be established, and their implementation must be supervised by the ICT security team with assistance from the inspectorate. The secrecy and safety of whistleblowers, whose actions may lead to information security disruptions. Organizations must also be firm in imposing sanctions on employees who disregard information security rules within the organization, as this could potentially jeopardize the security of the organization's data and systems [18]. Information security is a critical priority that demands serious attention. With the existence of consequences for negligence, organizations can create a culture that is more responsible for data protection and ensure that every employee plays an active role in maintaining the organization's cybersecurity.

Organizations also need to carry out socialization to help employees understand the importance of taking preventive measures to avoid potential negative consequences from their actions [19]. We can encourage employees to restrict others' access to their office and personal devices and to regularly back up their data to avoid data loss or theft. Lastly, organizations should conduct periodic ISA measurements, as security awareness assessments should not be a one-time event. Organizations should continuously evaluate employees' understanding of information security [16]. In addition, there may be new employees whose level of ISA has not yet been measured. When implementing the next security awareness program, it is necessary to separate the groups based on their target audiences. The separation of these groups can be based on IT or non-IT units where the audience's knowledge of security and information security culture differs [17].

The findings of this study indicate that the level of ISA among employees at ABC Agency is satisfactory overall, although the Internet Use dimension requires targeted attention. This aligns with our initial hypothesis that employees would demonstrate a good level of ISA, influenced by the agency's existing training and security policies. However, it also highlights a significant area for improvement, as in previous studies, such as those by Alshaikh et al. [10], have shown that robust ISA training programs are necessary to bridge gaps in employee knowledge, particularly in technology-heavy domains. When comparing our results to related research, it is evident that while organizations invest heavily in technological defenses, human factors remain a critical vulnerability in data security [4], [5]. Our research confirms these findings, proving that despite satisfactory general awareness, specific dimensions like Internet Use do not meet the desired security compliance standards. This suggests that ISA programs should not only focus on general awareness but also specifically address common pitfalls associated with internet usage. By identifying these weaknesses, our study contributes to the broader understanding of ISA in public sector organizations handling sensitive data, reinforcing the necessity for tailored awareness initiatives that respond to these contexts' unique challenges. Consequently, ABC Agency must implement focused programs that enhance understanding and responsible behavior surrounding internet usage to fortify its overall security posture.

This research has limitations in terms of sample diversity. The respondents in this study were not separated between IT and non-IT employees, so the researchers do not know in detail the information security awareness of employees who do not have an IT background. Future research should consider separating the target respondents from the IT and non-IT units.

4. Conclusions

This study provides helpful information about the level of ISA among employees at ABC Agency. It shows that their overall level of awareness is satisfactory, but there are some problems in the Internet Use dimension. These results support our original theory that ongoing ISA training is necessary and show how important it is to focus educational efforts on specific areas that need attention. This study has important implications for both information security and the agency itself. It shows that security training needs to be more rounded, going beyond basic knowledge and including useful skills for everyday online activities. The results also show that regular checks of ISA should be an important part of the agency's cybersecurity plan. This will help create a culture of constant security awareness. This study opens avenues for future research, such as exploring the effectiveness of differentiated training programs tailored to IT and non-IT employees. By addressing these considerations, the ABC Agency can mitigate potential security risks posed by human factors and serve as a model for other public sector organizations facing similar challenges. Enhancing ISA at ABC Agency will contribute to a more assertive cybersecurity posture, safeguarding sensitive data and ensuring compliance with relevant regulations. This study could also change how information security is handled in the public sector. It could persuade other government agencies to take similar steps and regularly check their employees' information security knowledge. More broadly, the increase in information security awareness in public institutions will benefit the organizations internally and have positive implications for society. We anticipate improving public behavior towards data security and privacy when employees become more aware of information security risks. This can reduce cybercrime incidents and increase public trust in institutions that manage sensitive information.

References

[1] A.-S. I, W. Yassin, N. Tabook, R. Ismail, and A. Ismail, “Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, 2022, doi: 10.14569/IJACSA.2022.0130855.

[2] A. Skatova, R. McDonald, S. Ma, and C. Maple, “Unpacking privacy: Valuation of personal data protection,” *PLoS One*, vol. 18, no. 5, p. e0284581, May 2023, doi: 10.1371/journal.pone.0284581.

[3] “UU No. 27 Tahun 2022.” Accessed: Oct. 21, 2024. [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[4] M. Neri *et al.*, “Understanding information security awareness: evidence from the public healthcare sector,” *Information & Computer Security*, Aug. 2024, doi: 10.1108/ICS-04-2024-0094.

[5] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, “Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior,” *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

[6] W. P. Wong, H. C. Tan, K. H. Tan, and M.-L. Tseng, “Human factors in information leakage: mitigation strategies for information sharing integrity,” *Industrial Management & Data Systems*, vol. 119, no. 6, pp. 1242–1267, Jan. 2019, doi: 10.1108/IMDS-12-2018-0546.

[7] Badan Siber dan Sandi Negara, “Lanskap Keamanan Siber Indonesia Tahun 2023,” 2024.

[8] M. C. De Maggio, M. Mastrapasqua, M. Tesei, A. Chittaro, and R. Setola, “How to Improve the Security Awareness in Complex Organizations,” *European Journal for Security Research*, vol. 4, no. 1, pp. 33–49, 2019, doi: 10.1007/s41125-017-0028-2.

[9] J. Abawajy, “User preference of cyber security awareness delivery methods,” *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

[10] M. Alshaikh, S. Maynard, A. Ahmad, and S. Chang, *An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations*. 2018. doi: 10.24251/HICSS.2018.635.

[11] M. M. Chumaera, Safitri, and M. A. Ayu, “Assessing Students’ Information Security Awareness through the Knowledge, Attitude, and Behavior Model,” in *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, Jul. 2022, pp. 1–6. doi: 10.1109/ICCED56140.2022.10010455.

[12] P. K. Sari, Candiwan, and N. Trianasari, “Information security awareness measurement with confirmatory factor analysis,” in *2014 International Symposium on Technology Management and Emerging Technologies*, 2014, pp. 218–223. doi: 10.1109/ISTMET.2014.6936509.

[13] 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)*, IEEE, Oct. 2020, pp. 1–7. doi: 10.1109/CITSM50537.2020.9268795.

[14] Y. Gardenia and A. G. Gani, “Cybersecurity Awareness Model with Methods: Analytical Hierarchy Process and Structural Equation Model,” *ICST Transactions on Scalable Information Systems*, vol. 11, Aug. 2024, doi: 10.4108/eetsis.6931.

[15] D. S. Hermawan, F. Setiadi, and D. Oktaria, “Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency,” in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, 2022, pp. 174–179. doi: 10.1109/ICoSEIT55604.2022.10029989.

[16] H. Ernita, Y. Ruldeviyani, D. Nurul Maftuhah, and R. Mulyadi, “Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 4, pp. 577–584, Aug. 2022, doi: 10.29207/resti.v6i4.4170.

[17] 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 *2019 5th International Conference on Computing Engineering and Design (ICCED)*, 2019, pp. 1–5. doi: 10.1109/ICCED46541.2019.9161120.

[18] Rosihan and A. N. Hidayanto, “Measurement of Employee Information Security Awareness: A Case Study at an Indonesian Correctional Institution,” in *2022 1st International Conference on Information System & Information Technology (ICISIT)*, Jul. 2022, pp. 318–323. doi: 10.1109/ICISIT54091.2022.9872988.

[19] H. Kruger and W. Kearney, *Measuring Information Security Awareness - A West Africa Gold Mining Environment Case*. 2005.

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

[21] A. Joshi, S. Kale, S. Chandel, and D. Pal, “Likert Scale: Explored and Explained,” *Br J Appl Sci Technol*, vol. 7, no. 4, pp. 396–403, Jan. 2015, doi: 10.9734/BJAST/2015/14975.

[22] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2017.

[23] N. M. Janna and H. HERIANTO, “Konsep Uji Validitas Dan Reliabilitas Dengan Menggunakan SPSS,” Jan. 22, 2021. doi: 10.31219/osf.io/v9j52.

[24] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” *Comput Secur*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.

[25] T. L. Saaty, “How to make a decision: The analytic hierarchy process,” *Eur J Oper Res*, vol. 48, no. 1, pp. 9–26, Sep. 1990, doi: 10.1016/0377-2217(90)90057-I.

[26] D. Panda, B. Kishore Mishra, and K. Sharma, "A Taxonomy on Man-in-the-Middle Attack in IoT Network," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, IEEE, Dec. 2022, pp. 1907–1912. doi: 10.1109/ICAC3N56670.2022.10074170.

[27] D. Septianto, Lukas, and B. Mahawan, "USB Flash Drives Forensic Analysis to Detect Crown Jewel Data Breach in PT. XYZ (Coffee Shop Retail - Case Study)," in *2021 9th International Conference on Information and Communication Technology (ICoICT),* IEEE, Aug. 2021, pp. 286–290. doi: 10.1109/ICoICT52021.2021.9527419.

[28] S. Alder, "Updated NIST Password Guidelines Replace Complexity with Password Length," The HIPAA Journal. Accessed: Nov. 27, 2024. [Online]. Available: https://www.hipaajournal.com/nist-password-guidelines-update-2024/

[29] M. Kulkarni *et al.*, "Mitigating Email Phishing: Analytical Framework, Simulation Models, and Preventive Measures," in *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Apr. 2024, pp. 1459–1464. doi: 10.1109/ICCSP60870.2024.10543325.

[30] A. Kusumawati, "Information Security Awareness: Study on a Government Agency," in *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2018, pp. 224–229. doi: 10.1109/SIET.2018.8693168.