VOL. 9. NO. 2 FEBRUARY 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v9i2.4163

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

MEASUREMENT OF EMPLOYEE INFORMATION SECURITY AWARENESS: CASE STUDY AT FINANCIAL INSTITUTION

Friendly Nur Shakti[1*], Achmad Nizar Hidayanto[2]

Magister of Technology Information[1,2]
Universitas Indonesia[1,2]
https://www.ui.ac.id/[1,2]
friendly.nur11@ui.ac.id[1*], nizar@cs.ui.ac.id[2]

(*) Corresponding Author

Abstract—*The lack of awareness regarding information security among employees in financial institutions can have detrimental impacts on both customers and the institution itself, both financially and in terms of trust. Therefore, this research aims to assess the information security awareness at PT XYZ, a financial institution, in order to identify the existing level of awareness, which will be used to provide recommendations. The method applied in this research is quantitative, using a questionnaire as a tool for data collection and distribution with a voluntary sampling technique among PT XYZ employees concerning their awareness of information security. The assessment of information security awareness covers 8 specific aspects, with 7 of them drawing sources from HAIS-Q and another 1 referring to the KAMI Index, using the Analytic Hierarchy Process (AHP) for weighting each area. The total number of respondents participating in this research is 52. The research results affirm that PT XYZ employees have a positive awareness of information security, indicating that there are no urgent actions needed at present. However, there are specific areas with potential for improvement, hence recommendations are provided to enhance and sustain information security awareness among employees.*

Keywords: *AHP, employee awareness, financial institution, HAIS-Q, information security awareness, KAMI index.*

Intisari— *Kurangnya kesadaran akan keamanan informasi pada karyawan di lembaga keuangan dapat membawa dampak merugikan baik bagi nasabah maupun institusi itu sendiri, baik dari segi finansial maupun kepercayaan. Oleh karena itu, penelitian ini bertujuan untuk menilai kesadaran keamanan informasi di PT XYZ, sebuah lembaga keuangan, guna mengidentifikasi tingkat kesadaran yang ada, sehingga hasilnya akan digunakan untuk memberikan rekomendasi. Metode yang diterapkan dalam penelitian ini bersifat kuantitatif, dengan menggunakan kuesioner sebagai alat pengumpulan dan penyebaran data dengan teknik pengambilan sampel sukarela kepada karyawan PT XYZ mengenai kesadaran akan keamanan informasi. Penilaian kesadaran akan keamanan informasi mencakup 8 aspek fokus, 7 di antaranya mengambil sumber dari HAIS-Q dan 1 lainnya mengacu pada Indeks KAMI yang pembobotannya menggunakan proses Analytic Hierarchy Process (AHP). Jumlah total responden yang berpartisipasi dalam penelitian ini sebanyak 52 responden. Hasil penelitian menegaskan bahwa para karyawan PT XYZ memiliki kesadaran akan keamanan informasi yang positif, mengindikasikan bahwa saat ini tidak ada tindakan mendesak yang perlu diambil. Meski demikian, terdapat area-area tertentu yang berpotensi untuk ditingkatkan, sehingga rekomendasi diberikan guna meningkatkan dan mempertahankan kesadaran akan keamanan informasi di kalangan karyawan.*

Kata Kunci: *AHP, kesadaran karyawan, lembaga keuangan, HAIS-Q, kesadaran akan keamanan informasi, indeks KAMI.*

INTRODUCTION

During a pandemic, access to financial services is very important, especially for people who need financing, especially in locations far from financial access, such as banks or other financial institutions, to maintain their businesses. This accelerating push towards digitalization of financial services may be a response for digital financial inclusion given the problems posed by the pandemic. Digital finance, especially cashless mobile money, has proven to be the foundation of financial inclusion in developing countries for individuals who are isolated and financially poor [1]. Apart from digitizing its financial services, a financial company must also adapt by initiating work from home as a mitigation measure against the spread of the pandemic virus. Employees who work from home have access to many systems, but companies still need to ensure the security and

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti
No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 9. NO. 2 FEBRUARY 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i2.4163

safety of employee and company data and digital assets are maintained. At the same time, information security is also a concern because companies find it difficult to control security on the devices employees use when working from home. Privacy and security issues have been highlighted [2] in the reliance on information systems and applications during the pandemic because employees have become targets of fraudsters who have the potential to access their computer devices, for example with phishing emails that attach malware to steal sensitive data.

The human factor in information security is a very important factor. According to [3] most companies have a tradition of continuing to ignore the human factor as the main contributor to security breaches because they choose to focus more on improving and developing technology. Research [4] reveals that when companies deal with user perceptions of information security, those perceptions are influenced by a number of factors, including awareness, knowledge, control, severity, and contingency, all of which have an impact on how users behave and make decisions. Therefore, researching the information security of a company based on human factors needs to be done in order to measure the level of awareness of information security among employees in the company.

Information security awareness is known as a condition of knowledge and awareness that is often found to have an impact on security compliance behavior. Research [5] shows the results that security policies in a company or organization and employee knowledge of information systems are influential information security awareness. Based on research [6] the notion of information security awareness has two aspects. The first aspect concerns the extent to which employees know that they are safe from information security behavior according to what has been described in the rules, policies and guidelines that have been made by the companies where they work. While the second aspect concerns the extent to which the employee has the commitment and behavior in accordance with what has been described in the information security rules, policies and guidelines in practice.

According to [7], due to the information-intensive nature of the financial business, financial institutions are placing greater emphasis on cyber risks and cyber threats. [8] also explained that one of the significant information security risks faced by financial institutions globally is hackers. Because financial institutions rely heavily on IT to carry out their fundamental business operations, they face various information security threats. Information security in Indonesia has been referred to in OJK regulations. in the commercial banking sector [9] and the non-bank financial sector [10], where both have stated that institutions are required to ensure information security is carried out on aspects of technology and aspects of human resources in the process of using technology aimed at maintaining the confidentiality, integrity, and availability of information contained and managed.

PT XYZ is a company operating in the financial sector in Indonesia, although in this context, researchers have disguised it as "PT XYZ" to maintain confidentiality. In 2022, it was found that illegal use of account access by unknown persons resulted in a loss of more than 60 million rupiah. Not only that, 21 other accounts have also been found that have not changed their passwords, making them vulnerable to fraud. Other cases have also been found, such as sharing user access, where an employee's user access is borrowed by another employee, and granting user access and carrying out the password through a chat group where, in the group, there are other people besides the two of them. Research [11] defines that information security incidents are related to human error, which is deliberately taking actions that result in failure to complete tasks to achieve the desired results due to a vulnerability. This human error can cause violations of the confidentiality of information through technical security failures that can disrupt the business operations of an organization or a particular individual. In an effort to increase knowledge related to information security awareness, PT XYZ has also carried out a socialization program related to posting information about security awareness on the CRM application so that PT XYZ employees can know the importance of security awareness. Materials that have been provided range from phishing emails, use of USB drives, clean and clear desks, provisions for using passwords, logical access security, use of public hotspots, use of VPNs, knowledge related to malware, social engineering, use of G-drives, data privacy, and ransomware. With this socialization, it is hoped that PT XYZ's employees will increase awareness of information security. The effectiveness of the application of information security programs cannot be achieved without the awareness of the employees of the organization itself [12].

A lot of research related to information security awareness has been carried out, research [13] which examine security awareness for smartphone users. Research [14] also conducted survey-based research on security awareness or behavior on social media. Kruger and Kearney in [6] using the KAB model, namely Knowledge, Attitude and Behavior. The KAB model has also been used in studies [15]. Each dimension has several focus areas that will be used to measure the level of information

security awareness. The KAB model developed by Kruger and Kearney that also used in [6] is the most frequently used model. The KAB model has also been used in research to measure employee information security awareness in healthcare institutions [16], also in elementary and highschool in Netherlands [15], with average or medium results, indicating that further action and supervision are required. But most of these studies measure in non-financial organizations and there is still very little research to measure the level of information security awareness, especially during a pandemic and financial digitalization for cases in financial institutions, even though during a pandemic and financial digitalization like this the emphasis on information security awareness on employees from financial institutions is greater because rely heavily on information technology in carrying out their business processes. The contribution of this research also includes research that measures information security awareness in the non-bank financial sector, where researchers currently have not found any research in that sector, and also research related to the combination of the HAIS-Q and KAMI Index, which are based mainly on non-existent operating system factors. on HAIS-Q.

To find out the level of information security awareness at PT XYZ, this research will design a measurement of the right level of information security awareness that will be implemented for PT XYZ employees in order to find out the level of information security awareness of PT XYZ employees so that recommendations can be made based on the measurement results as a reference for improvement. The model used in this study is the KAB model using the HAIS-Q focus area instrument combined with the KAMI Index to measure the level of information security awareness.

[15] has refined the information security awareness survey questions used to create the Human Aspects of Information Security Questionnaire (HAIS-Q). In HAIS-Q there are seven focus areas which include password management, email use, internet use, social networking use, mobile computing, information handling and incident reporting which have been tried in his research. KAMI Index is derived from the general understanding of the level of development of existing information security work programs within a company or institution. It is based on Standard SNI ISO/IEC 27001:2009, which includes: 1) Role of ICT/Level of Interest; 2) Governance; 3) Risk Management; 4) Information Security Framework; 5) Asset Management; and 6) Information Technology and Security [17]. In this study, only one area will be used from the KAMI Index, which is the Information Technology and Security area.

MATERIALS AND METHODS

Research Steps

This study consists of a comprehensive eight-step process, carefully designed to ensure the accuracy and reliability of research findings. The steps involved include identifying research problem, conducting literature review, determining research design/method, developing research instruments, collecting data, processing and analyzing data, creating recomendation, and making conclusion. Figure 1 visually depicts each step of the process. By following this structured approach, the study aims to ensure that all necessary aspects are covered and that the research findings are rigorous and reliable.

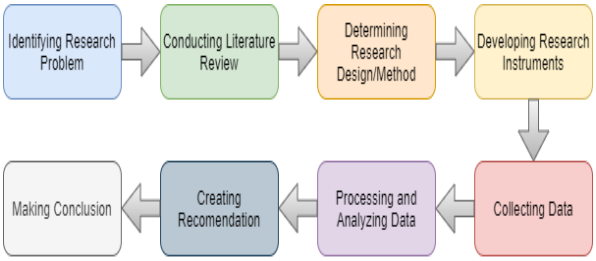


Figure 1. Research Steps

Adhering to this systematic framework, the study aims to ensure that every important aspect is adequately covered. This structured process not only enhances the depth of investigation but also encourages the production of rigorous and reliable research outcomes, serving as a crucial foundation for well-informed and robust conclusions and recommendations.

Research Instrument

The variables used in this study consist of three dimensions, namely knowledge which means what they know about information security, attitude which means how they feel about information security, and behavior model which means what they do on information security. These dimensions are collectively known as the KAB model, which provides a comprehensive framework for understanding information security awareness.

Researchers employed a set of 72 questions, sourced from the HAIS-Q and KAMI indexes, in their study. This approach enabled them to identify and assess knowledge, attitudes, and behavior across eight distinct focus areas within the realm of information security awareness. These focus areas, depicted in Figure 2 as the theoretical model, serve as the foundation for understanding the multifaceted aspects of information security.

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti
No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 9. NO. 2 FEBRUARY 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i2.4163

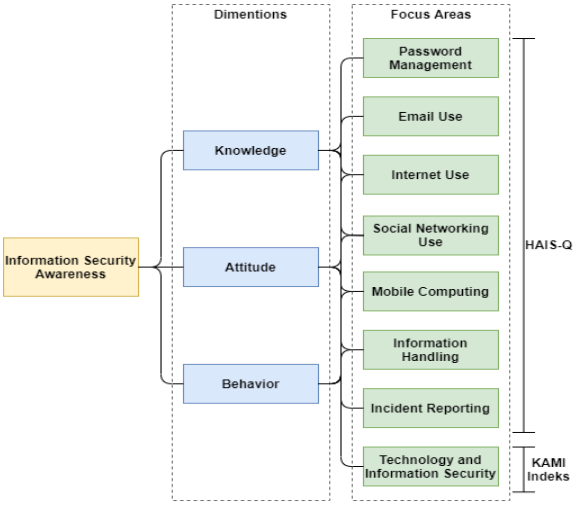


Figure 2. Theoritical Model

Each of these dimensions is subsequently subdivided into eight distinct information security focus areas, sourced from the HAIS-Q and KAMI Indexes. Furthermore, each of these focus areas is further subdivided into 24 individual sub-areas, as illustrated in detail in Table 1.

Table 1. Focus Areas and Subareas Adjusted with Company Condition

Focus Area	Subarea
Password Management	Changing password
	Sharing user and password
	Using strong password
	Write user and password
Email Use	Clicking on links in an email from known senders
	Clicking on links in an email from unknown senders
	Open attachments in emails from unknown senders
Internet Use	Downloading files
	Accessing suspicious sites
	Entering information in online
Social Networking Use	Account privacy settings
	Consider the consequences
	Posting about confidential work
Mobile Computing	Securing mobile devices
	Sending sensitive information over public Wifi
	Shoulder surfing
Information Handling	Disposing sensitive prints
	Insert removable media
	Leaving sensitive material behind
Incident Reporting	Report suspicious behavior
	Ignoring bad security behavioor by co-workers
	Report all incidents
Technology and Information Security	Use of technology in securing information assets
	Operating system

The three dimensions of the KAB model are included in the questionnaire approach. The knowledge dimension is examined in the first set of questions, the attitude dimensions in the second set, and behavioral factors in the third set. [15] used these three-dimensional questions and compared them to eight focus areas, including the seven focus areas from the HAIS-Q and the one focus areas from the KAMI Index. The research questions were asked sequentially, with short answers given using a Likert scale for each on a scale of 1 to 5, as shown in Table 2.

Table 2. Answer Scale Value

Scale Value	Description
1	Strongly Disagree
2	Disagree
3	Netral
4	Agree
5	Strongly Agree

To ensure accurate measurement of attitudes or opinions, a reverse scale will be used for negative questions. This means that responses to negative questions will be scored in the opposite direction to positive questions.

Table 3 shows an example of three questions posed in the using strong password subarea from each dimension in KAB model. The examples of questions in Table 3 ending with a "*" are examples of negative questions.

Table 3. Sample Question

Dimension	Question
Knowledge	A strong password is one that consists of uppercase letters, lowercase letters, numbers and symbols
Attitude	Use a password that is not too complicated to make it easier to remember*
Behavior	Using passwords that are related to personal matters such as birthdays or names*

Data Collection

This research was conducted at PT XYZ, which was conducted from January 2023 to February 2023. To collect data, surveys are generated using Google Forms, a user-friendly online tool that allows researchers to create and customize questionnaires quickly and easily. In the initial stage of this research, before the questionnaire is distributed to all employees, the researcher provided a questionnaire to three respondents with the aim of testing the questionnaire's readability. The results of this readability test were based on the feedback received from three respondents who participated in readability test. These improvements were implemented to ensure that the questionnaire is clear, concise, and easy to understand.

After conducting the readability test, the next step is to distribute the questionnaires to employees of PT XYZ. To achieve this, we will leverage the messaging application currently used by the office as a channel for distribution. This approach ensures that the questionnaire is easily accessible to employees, and encourages a higher response rate. To ensure that the data collected in this study truly reflects the perceptions and experiences of PT XYZ employees regarding information security awareness, the questionnaire was distributed through a voluntary and anonymous approach. By doing so, the collected responses will represent all employees of PT XYZ's security awareness. The questionnaire will be available for a period of two weeks, during which we will remind employees to complete it to increase the response rate.

Upon completion of the surveys by respondents, the collected responses are exported to Microsoft Excel for subsequent processing and analysis.

Measurement Steps

The initial step in assessing the weight of each area involves populating the area focus matrix pair. During the matrix selection process, the researcher evaluates defined focus areas and dimensions utilizing a graded scale. This scale comprises values: 1 denotes the least significant level, 3 corresponds to moderate importance, 5 signifies high importance, 7 represents very high importance, and 9 reflects the utmost level of importance that used in research [18]. By filling in the pairwise comparison focus areas, the AHP procedure will be used to find the weight of each focus area to measure information security awareness and dimensions.

The weight of each focus area and dimension that has been obtained will be used for the final calculation, resulting in the level of awareness of PT XYZ. The obtained values will be compared with the [6] scale, which has three levels: poor, moderate, and good. The scale, displayed as a color map, is used to intricately show the level of information security awareness in each target area, as depicted in Figure 3. The colors red and yellow indicate the "unsatisfactory" level, the "average" level, which may require improvement, and the "satisfactory" level, respectively.

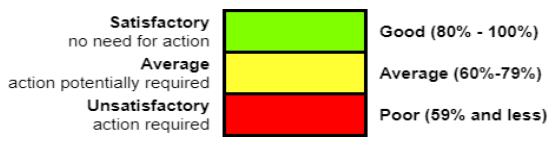


Figure 3. Information Security Awareness Color Scale [6]

RESULTS AND DISCUSSION

The results of the data collected through a questionnaire were analyzed to determine the level of information security awareness at PT XYZ, which would then be used as a reference in making recommendations.

Result of Data Collection

Before the questionnaire was distributed, the researcher randomly selected 3 respondents to test the readability of the questionnaire. After the readability test, the questionnaire was distributed through the channel and filled out by a total of 52 respondents. Respondents who have filled in will represent all employees of the organization where this research is conducted. After the data collection stage, the researcher performed a reverse value on negative questions in order to facilitate data processing.

Weighting Dimensions and Focus Areas

The weighting of the dimensions of the knowledge-attitude-behavior model and each focus area in this study was carried out using the AHP process to help prioritize the weights of each dimension and also each focus area. For this AHP calculation, we used an online software tool implemented by Goepel and also used in research [18]. The AHP process for each dimension can be seen in Figure 4.

Figure 4. Process of Weighting Dimensions

While the results of weighting dimensions are shown in Table 4.

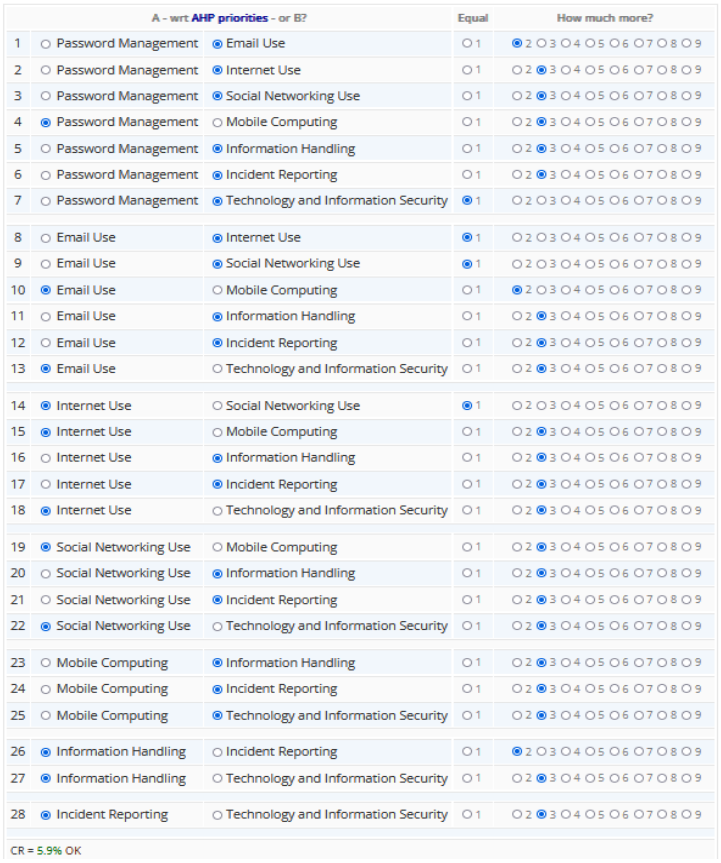
Table 4. Result of Weighting Dimensions

Dimension	Weight (%)
Knowledge	31.1
Attitude	19.6
Behavior	49.3

Meanwhile, the weighting process for each focus area can be seen in Figure 5.

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti
No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 9. NO. 2 FEBRUARY 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i2.4163



	A - wrt AHP priorities - or B?		Equal	How much more?
1	Password Management	Email Use	1	2 3 4 5 6 7 8 9
2	Password Management	Internet Use	1	2 3 4 5 6 7 8 9
3	Password Management	Social Networking Use	1	2 3 4 5 6 7 8 9
4	Password Management	Mobile Computing	1	2 3 4 5 6 7 8 9
5	Password Management	Information Handling	1	2 3 4 5 6 7 8 9
6	Password Management	Incident Reporting	1	2 3 4 5 6 7 8 9
7	Password Management	Technology and Information Security	1	2 3 4 5 6 7 8 9
8	Email Use	Internet Use	1	2 3 4 5 6 7 8 9
9	Email Use	Social Networking Use	1	2 3 4 5 6 7 8 9
10	Email Use	Mobile Computing	1	2 3 4 5 6 7 8 9
11	Email Use	Information Handling	1	2 3 4 5 6 7 8 9
12	Email Use	Incident Reporting	1	2 3 4 5 6 7 8 9
13	Email Use	Technology and Information Security	1	2 3 4 5 6 7 8 9
14	Internet Use	Social Networking Use	1	2 3 4 5 6 7 8 9
15	Internet Use	Mobile Computing	1	2 3 4 5 6 7 8 9
16	Internet Use	Information Handling	1	2 3 4 5 6 7 8 9
17	Internet Use	Incident Reporting	1	2 3 4 5 6 7 8 9
18	Internet Use	Technology and Information Security	1	2 3 4 5 6 7 8 9
19	Social Networking Use	Mobile Computing	1	2 3 4 5 6 7 8 9
20	Social Networking Use	Information Handling	1	2 3 4 5 6 7 8 9
21	Social Networking Use	Incident Reporting	1	2 3 4 5 6 7 8 9
22	Social Networking Use	Technology and Information Security	1	2 3 4 5 6 7 8 9
23	Mobile Computing	Information Handling	1	2 3 4 5 6 7 8 9
24	Mobile Computing	Incident Reporting	1	2 3 4 5 6 7 8 9
25	Mobile Computing	Technology and Information Security	1	2 3 4 5 6 7 8 9
26	Information Handling	Incident Reporting	1	2 3 4 5 6 7 8 9
27	Information Handling	Technology and Information Security	1	2 3 4 5 6 7 8 9
28	Incident Reporting	Technology and Information Security	1	2 3 4 5 6 7 8 9

CR = 5.9% OK

Figure 5. Process of Weighting Focus Areas

The results of weighting focus areas are shown in Table 5.

Table 5. Result of Weighting Focus Areas

Focus Area	Weight (%)
Password Management	6.5
Email Use	10.6
Internet Use	11.9
Social Networking Use	11.9
Mobile Computing	4.4
Information Handling	26.3
Incident Reporting	22.2
Technology and Information Security	6.3

After obtaining the weight percentages as shown in Table 5, these percentages will be used for the final calculations to determine the level of awareness.

Result of Analysis of Information Security Awareness

After collecting data and weighting the KAB model and all focus areas, the next step is to measure the level of information security awareness by processing the data with the help of a spreadsheet application. The results of measuring the eight focus areas and each of their dimensions, consisting of Knowledge (Knw), Attitude (Atd), and Behavior (Bhv) can be seen in Table 6.

Table 6. Result of Weighting Focus Areas

Focus Area	Knw	Atd	Bhv	Total
Password Management	82.50	66.92	82.98	79.68
Email Use	83.72	81.41	78.85	80.86
Internet Use	74.61	84.23	72.82	75.61
Social Networking Use	76.03	79.36	77.95	77.63
Mobile Computing	86.54	88.97	85.90	86.70
Information Handling	83.97	88.85	90.51	88.15
Incident Reporting	81.41	80.26	79.36	80.17
Technology and Information Security	82.35	80.38	87.31	84.10
Level of Awareness				**82.08**

The results of measuring information security awareness at PT XYZ are at a level of 82,08 which when viewed from scale [6], is at a good or satisfactory level and does not require further action. But if you look specifically at each focus area, out of the 8 focus areas, there are 3 focus areas consisting of the focus areas of password management, internet use, and social networking use, which are at an average level that potentially requires further action.

For the focus areas email use, mobile computing, information handling, incident reporting, and technology and information security, both knowledge and attitudes and behaviors are at

a satisfactory level where no further action is required. This is possible because socialization through media such as CRM or through company-wide announcements for awareness related to the focus area has been successful. Not only through socialization to increase information security awareness, but activities that are scheduled, such as "jumat bersih" related to the focus area of information handling are also carried out. This activity involves cleaning work desks where there are printed documents that can threaten the security of employees and the company.

Password management is at an average level and has a low score on the attitude dimension, especially in terms of changing passwords regularly. Employees react to this because they have a risk of forgetting passwords. Internet use also has a value at an average level, which lies in terms of downloading files to a laptop, where files downloaded to a laptop may carry risks such as viruses and the like that can be harmful. Then the last focus area that has an average level is social networking.

Recommendation

Based on [19], several factors have been mentioned that can increase information security awareness in private organizations, some of which are management support, because management support is the key thing that facilitates the need to develop information security awareness. The provision of training related to information security awareness also needs to be strengthened, and not only in the form of posts, because the awareness of employees to read these posts needs to be considered so that companies or organizations need to turn them into mandatory course programs that can also increase knowledge related to information security awareness, especially information technology. According to [19], the level of information security awareness of employees is positively influenced by their general knowledge of information technology because employees will be aware of information security issues in line with their knowledge of information technology.

Then, because PT XYZ is a company that adheres to a work from anywhere system, good control and monitoring are needed by the company. This is because employees who are used to working remotely have a lower level of information security awareness compared to those working in a corporate environment [5]. The information security governance structure also has a role to play in increasing information security awareness [19]. So that PT XYZ needs to have an information security department that can help increase employee information security awareness.

Another thing that is no less important is policy. This information security policy is a major factor as an effective way to increase employee information security awareness [19] and it must be ensured that the policies that have been made are known to all employees. The policies made must cover all focus areas, especially policies on changing passwords regularly, internet use, especially in downloading files and entering data related to personal and company data on a website page, as well as the use of social media, so that information security awareness for each focus area is at a satisfactory level.

CONCLUSION

The results of this study in measuring the level of information security awareness at PT XYZ, which is a company or financial institution, are at a level of 82,08 which when viewed from scale [6], is at a good and satisfactory level overall, and no further action is required. In maintaining and increasing the level of information security awareness, wse provide several recommendations related to management support, training programs, controls, and policies that are expected to have an impact on the eight focus areas.

For future research, there are several opportunities, which include validating the framework used in this study, which is used in a financial institution. Then, in further research, it is recommended to take further action in the form of interviews to validate the answers from employees so that more valid results are obtained. In addition, it would be very interesting if this research were conducted on all financial institutions in a country so that general statements or results were obtained that reflect the information security awareness of employees working in the country's financial institutions because financial institutions depend on information technology in their business processes and have an important role in society.

REFERENCE

[1] T. X. H. Tram, T. D. Lai, and T. T. H. Nguyen, “Constructing a composite financial inclusion index for developing economies,” *The Quarterly Review of Economics and Finance*, vol. 87, pp. 257–265, Feb. 2023, doi: 10.1016/J.QREF.2021.01.003.

[2] Y. K. Dwivedi *et al.*, “Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life,” *Int J Inf Manage*, vol. 55, p. 102211, Dec. 2020, doi: 10.1016/J.IJINFOMGT.2020.102211.

Accredited Rank 3 (Sinta 3) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No. 28/E/KPT/2019, September 26, 2019. Published by PPPM STMIK Nusa Mandiri

VOL. 9. NO. 2 FEBRUARY 2024
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v9i2.4163

[3] F. Schlackl, N. Link, and H. Hoehle, "Antecedents and consequences of data breaches: A systematic review," *Information & Management*, vol. 59, no. 4, p. 103638, 2022, doi: https://doi.org/10.1016/j.im.2022.103638.

[4] S. S. Ramalu, N. B. Z. Abidin, G. Nadarajah, and A. B. Anuar, "The Determinants of Risky Cybersecurity Behaviour: A Case Study Among Employees in Water Sector in Malaysia," *Journal of Law and Sustainable Development*, vol. 11, no. 12, p. e2706, Dec. 2023, doi: 10.55908/sdgs.v11i12.2706.

[5] H. Chen, Y. Zhang, S. Zhang, and T. Lyu, "Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention," *Educ Inf Technol (Dordr)*, vol. 28, pp. 1–34, Jan. 2023, doi: 10.1007/s10639-023-11771-z.

[6] J. Zhen, K. Dong, Z. Xie, and L. Chen, "Factors Influencing Employees' Information Security Awareness in the Telework Environment," *Electronics (Basel)*, vol. 11, p. 3458, Jan. 2022, doi: 10.3390/electronics11213458.

[7] A. Asmah and M. Kyobe, "A configurational analysis of IT governance: A study of the financial services sector in Ghana," *The Electronic Journal Of Information Systems In Developing Countries*, vol. 89, Jan. 2022, doi: 10.1002/isd2.12237.

[8] O. Gulyás and G. Kiss, "Impact of cyber-attacks on the financial institutions," *Procedia Comput Sci*, vol. 219, pp. 84–90, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.267.

[9] OJK, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum." 2022.

[10] OJK, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 4/POJK.05/2021 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Nonbank." 2021.

[11] M. Evans, Y. He, L. Maglaras, and H. Janicke, "HEART-IS: A novel technique for evaluating human error-related information security incidents," *Comput Secur*, vol. 80, pp. 74–89, Jan. 2019, doi: 10.1016/J.COSE.2018.09.002.

[12] M. Alshaikh, S. Chang, A. Ahmad, S. Maynard, and A. Alammary, "Embedding information security management in organisations: improving participation and engagement through intra-organisational Liaison," *Security Journal*, vol. 36, Jan. 2022, doi: 10.1057/s41284-022-00352-3.

[13] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers," *Journal of Systems and Software*, vol. 195, p. 111519, 2023, doi: https://doi.org/10.1016/j.jss.2022.111519.

[14] X. Wang, Y. Li, H. J. Khasraghi, and C. Trumbach, "The mediating role of security anxiety in internet threat avoidance behavior," *Comput Secur*, vol. 134, p. 103429, 2023, doi: https://doi.org/10.1016/j.cose.2023.103429.

[15] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the Netherlands," *Comput Educ*, vol. 186, p. 104536, 2022, doi: https://doi.org/10.1016/j.compedu.2022.104536.

[16] P. Nunes, M. Antunes, and C. Silva, "Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions," *Procedia Comput Sci*, vol. 181, pp. 173–181, 2021, doi: https://doi.org/10.1016/j.procs.2021.01.118.

[17] T. T. Wulansari and D. Novandi, "Evaluation of Information Security Management Using the KAMI Index Framework," in *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, 2022, pp. 173–177. doi: 10.1109/ICSINTESA56431.2022.10041714.

[18] A. Marcu, L. Moga, and E. Rusu, "Analysis of Some Essential Aspects Related to the Navigation Conditions on the Danube River," *Inventions*, vol. 6, p. 97, Jan. 2021, doi: 10.3390/inventions6040097.

[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, p. 102267, Jul. 2021, doi: 10.1016/J.COSE.2021.102267.