Accredited Ranking SINTA 2
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 on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 4 (2022) 577 - 584 ISSN Media Electronic: 2580-0760

Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ

[1]Halida Ernita, [2]Yova Ruldeviyani, [3]Desiana Nurul Maftuhah, [4]Rahmad Mulyadi
[1,2,3,4]Magister of Technology Information, Faculty of Computer Science, Universitas Indonesia
[1]halida.ernita@ui.ac.id, [2]yova@cs.ui.ac.id, [3]desiana.nurul@ui.ac.id, [4]rahmad.mulyadi11@ui.ac.id

Abstract

Bank handles private information like customer financial transactions and personal data. There was a 63% increase in cyberattacks attempted against Bank XYZ in 2021, and 1,323 attempted attacks on corporate email Bank XYZ. Therefore, implementing security awareness training for all employees is crucial for Bank XYZ. The information security awareness program must be assessed to determine the program's efficiency and the level of information security awareness among employees. Therefore, this study assesses the information security awareness at Bank XYZ, especially the Information Technology (IT) Directorate using the Human Aspect of Information Security Questionnaire (HAIS-Q) method. The findings of this study revealed that employees at Bank XYZ in the information security work unit had a "Good" level of awareness. In contrast, the results from other IT work units were "Medium". Based on the assessment results, Bank XYZ's security awareness strategy recommendation is to align awareness content with information security policies and procedures, use a variety of media awareness, and focus on the "Internet Use" and "Information Handling" awareness areas. As a way of determining the achievement of information security Key Performance Indicators (KPI), security awareness measurement must be done regularly, for example, once a year.

Keywords: information security awareness, information security awareness strategies, Human Aspect of Information Security Questionnaire (HAIS-Q), information security measurement, Knowledge Attitude Behaviour (KAB)

1. Introduction

The Covid-19 pandemic has accelerated digital transformation and transformed people's habits. People now use digital banking to conduct financial transactions, e-commerce to shop, work remotely from anywhere, and study using online resources. This circumstance encourages the expansion of digitization in the financial sector, particularly in banking. The increasing digitization trend has increased cyberattacks, particularly against financial institutions. The impact of cyberattacks can result in losses for the bank and its customers. Social engineering, processing failure, hardware failure, internal fraud, and cyberattacks are all high-risk areas in banking, according to the Banking Sector Risk Profile Report 2020 published by The National Cyber and Crypto Agency (BSSN) [1]. Indonesia's banking regulator is the Financial Services Authority (OJK). According to OJK Regulation No.38 of 2016, banks are obligated to guarantee information security is adequately implemented in terms of technology, people, and processes in the use of information technology [2].

Information security is concerned with ensuring data confidentiality, integrity, and availability. Information security risks are intrinsically tied to the people involved in the business process. People are the weakest link in the information security chain [3]. Employees are the most dangerous threat to information security in a company because their actions can significantly affect an organization's information system [4]. As a result, it's critical to conduct an information security awareness program on a regular basis to raise employee awareness of information security. The information security awareness program is expected to increase employees' knowledge of information security policies and procedures, as well as their attitude toward following those policies and procedures, resulting in better information security behaviour [5].

The main objective of security awareness is to ensure that computer users are aware of the risks associated with using technology, as well as understanding and abiding by security policies and procedures [5]. An information security awareness program in the bank is a complex preventive control, which needs to be

Accepted: 22-06-2022 | Received in revised: 09-08-2022 | Published: 22-08-2022

designed and implemented carefully to overcome employees' non-compliant behaviours related to information security policies [6].

Bank XYZ is a state-owned company with a big asset base and many customers across Indonesia [7]. The digital transformation that Bank XYZ is undergoing increases the risks of cyberattacks on information assets and sensitive company data. As a response, Bank XYZ established a dedicated work unit under the Directorate of Digital and Information Technology responsible for managing information security. The primary responsibility of the information security work unit is to ensure the company's implementation of information security, including conducting an information security awareness program. Based on Bank XYZ's annual security monitoring report, in 2021 there was an increase in cyberattack attempts by 63% from the previous year and there were 1,323 attempted attacks on corporate emails that were successfully detected [8]. As a response, it's necessary to verify that Bank XYZ employees are aware with information security.

Bank XYZ has implemented an information security awareness program for all employees that is updated regularly and uses various media and topics depending on the bank's risk profile. Posters, e-learning, email, webinars, and podcasts are all utilized to raise media awareness. Bank XYZ also runs a phishing campaign on a regular basis to evaluate employee awareness of the phishing threat. It is necessary to measure the programs that have been implemented to assess the effectiveness of information security awareness and ensure employees' awareness of information security. Measuring employee knowledge, attitude, and behaviour in the context of information security implementation is one method that can be applied. The Human Aspects of Information Security Questionnaire (HAIS-Q) is a tool that uses the Knowledge Attitude Behaviour (KAB) model to measure information security awareness [5]. The results of the questionnaire will be combined with the results of utilizing the Analytical Hierarchy Process (AHP) approach to determine the priority of security awareness areas from seven different focus areas. AHP helps decision makers to find the most appropriate solution by structuring the problem and ensure that all criteria and alternatives have been identified [9]. Then the result will be compared to the results of the phishing campaign to verify the level of awareness.

Previous studies have measured security awareness using HAIS-Q, such as measuring security awareness with case studies on digital wallet users which show average level scores therefore there are still many leaks in digital wallet users [10]. The other research on measuring awareness using HAIS-Q is a case study of measuring awareness in government institutions [11], and a case study at the judicial commission of the Republic of Indonesia [12]. Research on measuring awareness in the foreign affairs ministry was conducted using the AHP method, which is different from other research [13]. The banking sector is currently vulnerable to cyberattacks. This research develops security awareness strategies at Bank XYZ because no prior research has ever developed security awareness strategies and measurements in Indonesian banking institutions. The reason why Bank XYZ was selected as a case study is that it is one of the biggest banks in Indonesia, has a large customer base, and has a digital banking application, making it vulnerable to cyberattacks.

This study will provide insight into how Bank XYZ has implemented information security awareness, particularly among employees in the Digital and Information Technology (IT) Directorate. Because the study validated the awareness value based on a phishing campaign, it differs from prior research. This assessment is conducted to determine the level of understanding of employees directly involved with IT, and more particularly, employees in the information security work unit who are responsible for managing information security. This study compares awareness levels between employees in information security work units and employees in other work units at the IT Directorate. Employees in the information security organization are required to have a higher level of awareness than other IT employees. A security awareness strategy is developed based on the assessment results, with the goal of improving employee awareness of information security implementation.

2. Research Methods

There are eight processes in this research, as illustrated in Figure 1: problem identification, studying literature, determining the research method, creating research instruments, collecting data, process & analyzing data, creating recommendations, and creating a conclusion.

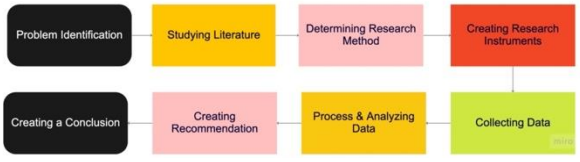

Figure 1. Research Step

2.1 Research Instruments

This research uses HAIS-Q as an information security awareness measurement tool for the employee at the IT Directorate of Bank XYZ. HAIS-Q has seven focus areas [5]. The information security awareness level will be calculated using distinct priorities and weights for each emphasis area. Determination of the weight of the focus area is carried out using the AHP method together

DOI: https://doi.org/10.29207/resti.v6i4.4170

with a team of experts from the IT Directorate of Bank XYZ. The HAIS-Q questions are divided into three categories: knowledge, attitude, and behaviour, which can indicate the relationship between employees' understanding of information security and their attitudes and daily behaviour. The HAIS-Q results will be compared to the phishing campaign results to validate the level of awareness.

This research uses a questionnaire based on the Human Aspects of Information Security Questionnaire (HAIS-Q) [5]. The questionnaire has 63 questions in English. The questions are organized into seven focus areas and sub-areas. This means that three questions are asked simultaneously for each sub-area, encompassing characteristics of knowledge (K), attitude (A), and behaviour (B). For example, the sub-section "using the same password" in the focus area "password management" consists of three consecutive questions, as shown in Table 1. The respondents chose an answer using a Likert Scale with a scale of 1 to 5, as shown in Table 2.

Table 1. KAB Question in the Password Management Focus Area

Aspect	Questions
Knowledge (K)	It's acceptable to use my social media passwords on my work account.
Attitude (A)	It's safe to use the same password for social media and work accounts.
Behaviour (B)	I use a different password for my social media and work accounts.

Table 2. Likert Scale

Scale	Category
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

This research uses an interview method with a group of specialists from Bank XYZ in complement to questionnaires. Senior managers from the Information Security work unit (ISC) of Bank XYZ's IT Directorate, who are responsible for information security governance, were interviewed. The purpose of the interview was to learn about the importance and weight of each focus area that is part of the information security awareness measurement. By comparing one focus area to another, the AHP method is used to determine weights. Table 3 displays the outcomes of this comparison.

Interviews with security specialists were also conducted to determine the risks and challenges that Bank XYZ encountered when implementing information security awareness. The execution of information security, particularly the information security awareness program at Bank XYZ, was also assessed through observations.

Table 3. Determining Area Focus Priority Scaling Using AHP

Criteria A	Criteria B	More Important A or B?	Scale (1-9)
Password	Email usage	A	7
	Internet usage	A	5
	Social media	A	5
	Mobile device	A	5
	Information handling	A	3
	Incident reporting	A	7
Email usage	Internet usage	B	7
	Social media	B	5
	Mobile device	B	3
	Information handling	B	7
	Incident reporting	A	5
Internet usage	Social media	A	5
	Mobile device	A	3
	Information handling	B	3
	Incident reporting	A	5
Social media	Mobile device	A	3
	Information handling	B	5
	Incident reporting	A	5
Mobile device	Information handling	B	5
	Incident reporting	A	3
Information handling	Incident reporting	A	7

2.2 Data Collection

Data was collected using a questionnaire distributed through an online form. The questionnaire has been filled out start from November 1 until November 20, 2021, with the target of employees in the IT Directorate of Bank XYZ. The target respondents were determined using the Slovin formula [14], as in formula 1.

$$n = \frac{N}{1+N\,(e^2)} \quad (1)$$

N = population size = 230, e = desired margin of error = 5%, n = number of samples = 146

There are 230 permanent employees with job positions ranging from supervisor to senior manager in the IT Directorate Bank XYZ. According to the formula's output, the minimum target sample respondents, who represent 6 IT work units, are 146 employees. Simple random sampling was used to choose this sample of responders since it is the least biased and provides the highest generalizability [15].

In addition, an interview process with a team of experts from the information security work unit was also conducted on November 22, 2021, to determine the priorities of the seven focus areas of awareness. Phishing simulation has been conducted from October 13 until October 30, 2021, with the target also including employees in the IT Directorate of Bank XYZ. Phishing simulation is sent to the employees using an open-source phishing simulation tool. This tool will record every employee that clicks the phishing link, submit data into the fake system or report this suspected email to the information security work unit.

DOI: https://doi.org/10.29207/resti.v6i4.4170

2.3 Methods / Techniques for Analyzing Data Methods

Based on the results of interviews with a team of experts from the information security work unit, a comparison of the focus areas was carried out, and it was determined which one was more priority, and the priority scale was from 1 to 9. The priority scale was determined as described in Table 4.

Table 4. Priority Scale

Importance	Definition	Explanation
1	Equal importance	Two elements contribute equity to the objective
3	Moderate importance	Experience and judgment slightly favour one element over another
5	Strong importance	Experience and judgment strongly favour one element over another
7	Very strong importance	One element is favoured very strongly over another is dominance is demonstrated in practice
9	Extreme importance	The evidence favouring one element over another is of the highest possible order of affirmation.

The first step taken to get the awareness value through the HAIS-Q method is to identify questions that have positive meanings and questions that contain negative meanings (question sentences contain negative sentences). For each positive question, a score of 1 is given for an answer on a scale of 4 and 5 and a value of 0 for an answer on a scale of 1 to 3. On the other hand, for a negative question, a score of 1 is given for an answer with a scale of 1 and 2 and a value of 0 for an answer with a scale of 3 up to 5.

After scoring 1 and 0, the next step is to add up all the answers with the values 1 and 0 for each question. The results obtained are used as a percentage value by dividing the total number of respondents. This number becomes the value for one dimension of the sub-area. To get the value of a focus area, then each value of the dimension in a focus area is multiplied by the weight of the dimension as defined by Kruger and Kearney in Table 5 [16].

Table 5. Dimension Weighted

Dimension	Weighted
Knowledge	30
Attitude	20
Behaviour	50

The next step is to calculate the awareness value by multiplying the results for each focus area (v_i) by the weight for each focus area (w_i) that has been made with the expert team previously using the calculation formula 2 [16]:

$$V(a) = \sum_{i=1}^{n} v_i\,(a)\,w_i \quad (2)$$

Based on the process of measuring the priority scale, weight is obtained for each focus with the results, which can be seen in Table 6.

Table 6. Weight For Each Focus Area

Focus Area	Weighted
Password	38.2 %
Email usage	3.80 %
Internet usage	16.30%
Information handling	24.90%
Mobile device	5.60%
Social media	8.90%
Incident reporting	2.30%

This weight will be used to calculate the awareness value from the results of the HAIS-Q questionnaire that has been distributed. The scores will be mapped into three levels, namely bad (bad), medium (medium), and good (good), which are based on the journal Kruger and Kearney [16] and can be seen in Figure 2.

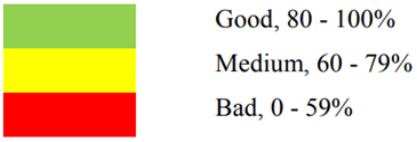

Figure 2. Security awareness level based on Kruger dan Kearney [16]

Each level of security awareness has different follow-ups. For the awareness level, "Bad" means awareness of information security is still very low and requires a lot of improvement. For the awareness level, "Medium" means that awareness of information security is quite good, but there are still some things that need to be improved. Meanwhile, the "Good" awareness level means that awareness of security is very good. The follow-up needed may only be in the form of strengthening or reminding activities that can be carried out periodically or other activities aimed at improving awareness of information security.

This research also compares the awareness value between the work unit responsible for information security, namely the information security work unit and the other IT work unit. The purpose of this comparison is to find out whether there are differences in awareness levels between the information security work unit and other IT work units. The awareness level between the information security work unit and the other IT work unit should be the same because one of the duties and responsibilities of the information security work unit is to disseminate and strengthen awareness of information security, for example, by broadcasting posters regarding information security to all employees of Bank XYZ. If the results of the awareness between the information security work unit and other work units are very different, it means that there is still a lack in the dissemination of information security awareness to all employees of Bank XYZ. This can also be used as an evaluation material and input for the IT Directorate of Bank XYZ in measuring the performance of the

DOI: https://doi.org/10.29207/resti.v6i4.4170

information security work unit, especially regarding information security awareness for Bank XYZ employees

3. Results and Discussions

The results of the questionnaire were analyzed to determine the level of awareness, which was then validated using the phishing simulation results. Thereafter, the data is used to develop Bank XYZ's security awareness strategy.

3.1 Questionnaire Result Analysis

Research questionnaires were distributed online to the employee at the IT Directorate of Bank XYZ. The total number of respondents who filled out the questionnaire was 147 people from six work units under the IT Directorate. Statistical data of respondents can be seen in Table 7.

Table 7. Respondent Statistical Data

Characteristics		Count	Percentage
Division	APP	65	44.21 %
	ISC	35	23.80 %
	EDM	14	9.52%
	DDB	4	2.72%
	ISG	20	13.60%
	INF	9	6.12%
Role	Supervisor	2	1.36%
	Officer	56	38.10%
	Assistant Manager	29	19.73%
	Manager	37	25.17%
	Senior Manager	23	15.65%
Education	S1	134	91.15%
	S2	13	8.85%

The results of the measurement of the average information security awareness level of the IT Directorate of Bank XYZ employees can be seen in Table 8. The total score obtained is 83.46%. Based on the category of information security awareness level by Kruger and Kearney [16], the awareness of employees is at the "Good" level.

In addition, the results of the questionnaire were also grouped specifically to obtain the awareness level of the employees in the information security work unit in Table 9 and the awareness level of other IT employees in Table 10. The awareness level of employees in the information security work unit is already at the "Good" level, although there is still a focus on the Use of Internet area, which has a "Medium" level. Meanwhile, the awareness level of employees other than in the information security work unit is still at the "Medium" level, and there is a focus on the Use of the Internet area rated "Bad".

Table 8. IT Directorate Information Security Awareness Score

Focus Area	K	A	B	Total awareness (Focus Area)
Password management	92.74	88.21	94.10	92.52
Email usage	81.86	83.45	86.39	84.44
Use of internet	58.28	81.18	59.86	63.65
Information handling	70.98	83.45	82.31	79.14
Mobile device	92.06	90.48	90.48	90.95
Use of social media	82.54	89.80	90.93	88.19
Incident reporting	86.17	82.99	79.37	82.13
Total awareness	80.19	85.84	84.47	83.46

Table 9. Information Security Work Unit Information Security Awareness Score

Focus Area	K	A	B	Total awareness (Focus Area)
Password management	95.24	97.14	98.10	97.05
Email usage	86.67	90.48	95.24	91.71
Use of internet	78.10	90.48	72.38	77.71
Information handling	80.00	89.52	84.76	84.29
Mobile device	98.10	93.33	94.29	95.24
Use of social media	88.57	97.86	96.19	94.24
Incident reporting	91.43	84.76	83.81	86.29
Total awareness	87.80	93.47	89.76	89.92

Table 10. Other IT Work Unit Information Security Awareness Score

Focus Area	K	A	B	Total awareness (Focus Area)
Password management	84.43	78.42	85.25	83.63
Email usage	73.77	74.59	76.78	75.44
Use of internet	47.81	71.86	51.37	54.49
Information handling	62.57	74.86	74.86	71.17
Mobile device	82.79	82.24	81.97	82.27
Use of social media	74.04	80.12	81.97	79.22
Incident reporting	77.60	75.68	71.58	74.21
Total awareness	71.44	76.62	76.03	74.77

DOI: https://doi.org/10.29207/resti.v6i4.4170

The average total awareness value of each focus area in Table 8, Table 9, and Table 10 are 83.46 for all employees in the IT Directorate of Bank XYZ, a value of 89.92 for employees in the information security work unit and a value of 74.77 for employees outside the information security work unit at the IT Directorate of Bank XYZ. The average value is generated by adding up all the total awareness values from each focus area and then dividing by the seven existing focus areas.

3.2 Phishing Simulation Result

The phishing simulation report result in Table 11 shows that only 4% of employees from IT Directorate Bank XYZ clicked a link in email phishing that was sent to the employee, and only 2% submitted data to the fake web phishing. It can be concluded that the awareness level in IT Directorate Bank XYZ in the "Good" level is valid.

Table 11. Phishing Simulation Result

Email sent	Clicked link		Submitted data		Email reported	
	People	%	People	%	People	%
401	15	4	7	2	6	1

3.3 Discussion

The bank is an industry that relies on customer trust. Banks manage customer data, so banks must secure customer data. The occurrence of data leakage can result in a loss of customer trust in the bank, which will ultimately have an impact on the bank's business. The following are recommendations for Bank XYZ's strategy to improve employee information security awareness based on measurement and observation that has been done in this research:

- Focus Area Awareness

The measurement results in the focus area "in use of the internet" has the lowest value, which means employees do not understand the risks of downloading files on a work computer, accessing dubious websites, and entering information on untrusted websites [5]. Based on observations that have been made in this research, Bank XYZ has not implemented restrictions on internet use in terms of technology, especially in the IT Directorate, so that internet usage activities can be carried out without limitations. Internet restrictions are only carried out at bank branch offices that are directly related to the transactional system and have a high risk. Therefore, an awareness program must be carried out to employees regarding the policy for using the internet, such as the policy about accessing websites and downloading files securely. Employees must make sure the website is secure, and the downloaded files do not contain malicious programs. Then employees must also be reminded not to enter information, either personal or company information, on an untrusted or not secure website.

The information must be carried out properly and following information security policies and procedures, both when processed, transferred, and when stored. Focus area information handling has a "Medium" awareness level. The employee still does not fully understand how to dispose and store of paper containing sensitive information and how to treat a removable media found in a public place [5]. The employee in the IT Directorate rarely use paper in doing their work; therefore, knowledge about how to treat hardcopy documents securely is low. Regarding the use of removable media, which is usually the entrance to ransomware, Bank XYZ has not restricted the use of removable media. However, Bank XYZ has already protected a PC or laptop by using antivirus software. This still poses a risk of cyberattack for the company because security in terms of technology is not yet optimal. Therefore, education and training for the employee in this focus area also need to be improved. The employee must understand how to manage information securely.

The very high risk of social engineering in the banking industry [1] also needs to be an additional focus area in raising awareness among employees. Social engineering uses psychological manipulation to trick victims into providing sensitive information. Employees who understand how to secure information can avoid social engineering risks.

- Content

Good security awareness programs should concentrate on reinforcing an organization's security policies, guidelines, and processes by disclosures of the required actions that employees should take in accordance with the security program [17]. Information security awareness must also be reviewed and updated regularly to remain relevant to the standards and regulations that apply in the industry. Security awareness and effective training programs explain how to behave (behaviour) are safe in handling information [18]. The information security awareness program is structured based on priority areas that have low values.

In designing security awareness programs, Banks and other information-centered organizations must create different concepts to reach all employees. The security awareness program must differentiate the roles of employees and the location of employees, such as head office employees and branch office employees. In addition, employees who handle critical information must receive a more intensive security awareness program [6]. Currently, security awareness content at Bank XYZ is the same for all employee roles.

- Media awareness

The knowledge of employees in the IT Directorate regarding information security is very important because it is directly related to the management of IT.

DOI: https://doi.org/10.29207/resti.v6i4.4170

Therefore, the security awareness program for IT employees is a crucial thing and must be carried out routinely and intensively, such as by conducting training related to information security. A security awareness program should consist of a specific kind of awareness message or communication channel that is related to the personality of each employee [6].

Information security awareness training those employees receive at work and during work hours is the most important factor that affects employees' awareness level [19]. Multi-channel information security training with the variation of platforms and media such as an intranet, email, online videos, posters, and flyers affect the security awareness level. Companies should also develop a reward program for employees who participate in security training. This reward, for example, prizes for employees with the highest quiz score or employees who are the most active when participating in training [17]. Gamifying compliance and training in cyber security is one strategy that has gained popularity among businesses that are concerned about cyber security [20]. Another method is to organize a competition or hands-on activity involving information security policies, with a prize for the winner.

- Measurement

Security awareness assessment is not something that is done just once. It must be done continuously to assess the level of understanding of employees and as a key performance indicator in the implementation of information security. Bank XYZ needs to evaluate why employees have not implemented information security, especially in the focus area of use of the internet and information handling, which have the lowest awareness score. Bank XYZ needs to apply penalties to employees who do not comply with the information security policies.

Information security awareness is only part of the overall implementation of information security, especially in the people aspect. Therefore, the development of information security in aspects of people, processes, and technology needs to be continuously carried out and improved. Bank XYZ needs to improve information security technology, especially in the focus area of use of the internet and information handling, which is still not optimal.

Employees' knowledge of information security policies and procedures greatly affects the knowledge, attitudes, and behaviour of employees towards information security policies and procedures, where the three will always be directly proportional. This shows that the higher the level of knowledge of an employee towards information security policies and procedures, their attitude towards information security policies and procedures will increase, and this will certainly result in much better information security behaviour.

4. Conclusion

Measurement of information security awareness level based on the KAB model and using HAIS-Q at the IT Directorate of Bank XYZ has been successfully carried out. Measurement was made on the implementation of knowledge, attitude, and behaviour of employees in 7 focus areas consisting of password management, email usage, use of the internet, use of social media, mobile devices, information handling, and incident reporting.

Based on the results of this research, it was found that the total security awareness level of each focus area of the information security work unit (ISC) employee was higher than other employees in the IT Directorate of Bank XYZ. Based on the average value of the three types of employees in the IT Directorate of Bank XYZ, it can be concluded that employee information security awareness in the IT Directorate of Bank XYZ is at the "Good" level. The focus area on the use of the internet and information handling areas still has an awareness level of "Medium" and needs to be improved.

The strategy to increase employee information security awareness at the IT Directorate of Bank XYZ is to create a comprehensive security awareness program. Security awareness content must align with information security policies and must be provided with attractive and various programs and media. Focus area awareness on the use of the internet and information handling areas that have the lowest value should be improved by conducting education and training intensively. The employee must be socialized about the policy for using the internet, specifically the policy about accessing websites and downloading files from the internet. The employee also needs an awareness program about how to dispose of and store paper containing sensitive information and how to treat a removable media found in a public place.

The higher the level of knowledge of an employee towards information security policies and procedures, their attitude towards information security policies and procedures will increase, and this will certainly result in much better information security behaviour. Therefore, it is necessary to carry out an information security awareness program on a regular and ongoing basis, using different methods and media. The employee awareness assessment must be carried out periodically, for example, in an annual period, as a method to determine the achievement of the information security Key Performance Indicator (KPI).

It is necessary to conduct further research that measures the effectiveness of the type of media used on the value of security awareness. In addition, there is also a need to create a standard that can be used by the Financial

DOI: https://doi.org/10.29207/resti.v6i4.4170

Services Authority to assess the security awareness level of banking companies.

Reference

[1] BSSN, "The National Cyber and Crypto Agency - Risk Profile Banking Sector," 2020. [Online]. Available: https://cloud.bssn.go.id/s/2kr268f6FHPAYoZ#pdfviewer.

[2] OJK, "Financial Services Authority Number 38 of 2016 Concerning Risk Management in the Use of Information Technology," 2016, [Online]. Available: https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK MRTI.pdf.

[3] Z. (Justin) Zhang, W. He, W. Li, and M. Abdous, "Cybersecurity awareness training programs: a cost–benefit analysis framework," *Ind. Manag. Data Syst.*, vol. 121, no. 3, pp. 613–636, 2021, doi: 10.1108/IMDS-08-2020-0462.

[4] N. A. A. Md Azmi, A. P. Teoh, A. Vafaei-Zadeh, and H. Hanifah, "Predicting information security culture among employees of telecommunication companies in an emerging market," *Inf. Comput. Secur.*, vol. 29, no. 5, pp. 866–882, 2021, doi: 10.1108/ICS-02-2021-0020.

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

[6] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, no. May 2018, pp. 145–159, 2017, doi: 10.1016/j.cose.2017.04.009.

[7] PT.Bank XYZ, "Anual Report Bank XYZ 2021," 2021.

[8] PT.Bank XYZ, "Cyber Attack Trend Bank XYZ , Annual Report 2021." 2021.

[9] E. Mu and M. Pereyra-Rojas, *Practical Decision Making using Super Decisions v3 : An Introduction to the Analytic Hierarchy Process*. 2018.

[10] A. L. Fadhilah, Y. Ruldeviyani, R. Prakoso, and K. F. Arisya, "Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1077, no. 1, p. 012003, 2021, doi: 10.1088/1757-899x/1077/1/012003.

[11] E. A. Puspitaningrum, F. T. Devani, V. Q. Putri, A. N. Hidayanto, Solikin, and I. C. Hapsari, "Measurement of employee information security awareness: Case study at a government institution," *Proc. 3rd Int. Conf. Informatics Comput. ICIC 2018*, pp. 1–6, 2018, doi: 10.1109/IAC.2018.8780571.

[12] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, "Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia," *Adv. Sci. Technol. Eng. Syst.*, vol. 5, no. 3, pp. 501–509, 2020, doi: 10.25046/aj050362.

[13] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, "Measurement of Employee Information Security Awareness Using Analytic Hierarchy Process (AHP): A Case Study of Foreign Affairs Ministry," *2018 Int. Conf. Comput. Eng. Des.*, pp. 52–56, 2018, doi: 10.1109/ICCED.2018.00020.

[14] T. P. Ryan, *Sample Size Determination and Power*. 2013.

[15] U. Sekaran and R. Bougie, "Research Methods for Business (7th Edition)," 2016, [Online]. Available: www.wileypluslearningspace.com.

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

[17] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *J. Organ. Comput. Electron. Commer.*, vol. 29, no. 4, pp. 249–257, 2019, doi: 10.1080/10919392.2019.1611528.

[18] M. Nieles and K. Dempsey, "NIST Special Publication 800-12 Revision 1, An Introduction to Information Security," *NIST Spec. Publ.*, pp. 1–101, 2017, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[19] M. Pattinson, M. Butavicius, K. Parsons, and A. Mccormac, "Managing information security awareness at an Australian bank : a comparative study," vol. 25, no. 2, pp. 181–189, 2017, doi: 10.1108/ICS-03-2017-0017.

[20] G. Kemper, "Improving employees' cyber security awareness," *Comput. Fraud Secur.*, vol. 2019, no. 8, pp. 11–14, 2019, doi: 10.1016/S1361-3723(19)30085-5.

DOI: https://doi.org/10.29207/resti.v6i4.4170