Assessment of Security Awareness Perception on Indonesian Media Industry

Tegar Pratama Putra1,a) and Nilo Legowo2,b)

1Information System Management Department, Bina Nusantara University, Jakarta, Indonesia

2Master of Information System Management Department, Bina Nusantara University, Jakarta, Indonesia

a) Corresponding author: tegar.putra@binus.ac.id

b) nlegowo@binus.edu

**Abstract.**  The involvement of organizational members can provide positive or negative contributions to the information security performance of an organization. Therefore, the organizations need a program covering human involvement in information security that allows them to provide a positive contribution. A security awareness program offers a solution to convey the relevance of the information to the organization's needs. However, the organizations need a solution to know the perceptions of organizational members that can be used to evaluate and enhance the security awareness program. The study aimed to delve deeper into organizational members perspectives on the security awareness program focusing on knowledge, attitude, and behavior (KAB) dimensions, along with other vital focus areas within the research object of an Indonesian media organization. Overall, organizational members have an adequate understanding of the security awareness program. The results can be described by considering the knowledge, attitude, and behavior (KAB) dimensions, as well as the focus areas such as password management, internet use, e-mail use, social media use, mobile devices, information handling, and incident reporting. These findings can also be used to offer suggestions for organizations to enhance the security awareness program. The studies are anticipated to provide the ­organizations with solutions to their organizational challenges. Future studies can be carried out by considering cyber fatigue elements in organizational members and incorporating other information security aspects that can be utilized in the security awareness program.

**Keywords:** Assessment, Knowledge Attitude Behavior, HAIS-Q, Media Industry, Security Awareness.

# INTRODUCTION

Information security offers protection against security threats in the digital era. It is defined as a strategic approach to map the information security threats and risks that impact confidentiality, integrity and {Zammani, 2021 #1}{Khando, 2021 #9}{Zammani, 2021 #1} availability [1]. An attacker's target in security might threaten an individual or an organization [2]. Information security management requires knowledge, expertise, commitment, willingness, and cooperation between individuals and teams in developing information security components [3]. Additionally, other variables such as knowledge sharing, collaboration, intervention, and experience also influence a person's attitude toward implementing positive behavior [4]. These variables provide convenience and a broader perspective for management when developing information security components in organizations. Information security management also needs to consider the development of information security policies that are not biased or open to multiple interpretations [5].

In securing assets or information, human involvement can be achieved by asking for support from all members of the organization for the presence of information security. This support is the biggest component influencing the success of information security [6]. In addition, with organizational members’ support, it is expected to enhance the performance of information security [7]. Even though the organizations have seen a positive stigma from involving their members, they also encounter the challenge of negative stigma from the members during the implementation process. Information security is considered as an obstacle and disrupts the comfort of organizational members when carrying out business processes [8]. This happened due to technical failures that are less appropriate and adequate in protecting assets and information [9]. Therefore, supporting strategies are needed by the organizations to minimize that negative stigma. Supporting strategies that can be developed in the form of policies and programs related to individual awareness of information security [10]. Additionally, security programs can be used to reduce human error and enhance the value in information security assessments [8].

Security awareness programs propose solutions to manage human involvement in information security. It will be an important step for organizations to involve organizational members who have varying levels of expertise and technical knowledge [11]. Additionally, security awareness programs will ensure organizational members know their roles and responsibilities regarding the policies, threats, and risks [3]. All organizational members should be given a proper program in the form of training and education to reduce human error that can result in a security threat [12].

The security awareness program that has been implemented can be evaluated to overview the effectiveness of this program. The organizations should be cautious of their organizational members behavior and variables that affect the work productivity [13]. As a result, supervision in the form of assessment offers a solution for determining the level of compliance of the organizational members [14]. In addition, the assessment will determine the positive or negative perceptions of the organizational members, which can be used in the development of information security guidelines and security awareness programs [15]. Having an assessment for each organizational member is not only limited to their knowledge and behavior, but also needs to consider their values, beliefs and attitudes toward information security [16]. The assessment scale must ensure collected data are relevant to the research topic, does not omit crucial information and can be reproduced [17]. When conducting this assessment, the organizations should assure the accuracy of the measurements to prevent the ineffectiveness of the security awareness solutions [18].

Attributed to those descriptions, it is necessary to assess the organizational members in the security awareness program. So that, exploration of the research objects will be conducted. This exploration indicates that an Indonesian organization that is involved in the media sector has implemented a security awareness program. By conducting the interviews with information security management, it was stated that there were obstacles in the overview of the perceptions of the organizational members after the program was running. Consequently, the interview results presented its relevance, which indicated that the organization could be used as a research object. A comprehensive and empirical assessment from the perspective of non-technical individuals should be carried out in information security management [11]. The assessment could analyze the factors and collect user facts about their capabilities and limitations [5]. The following study aimed to see the perceptions of the respondents on the research object and provide recommendations based on the assessment results.

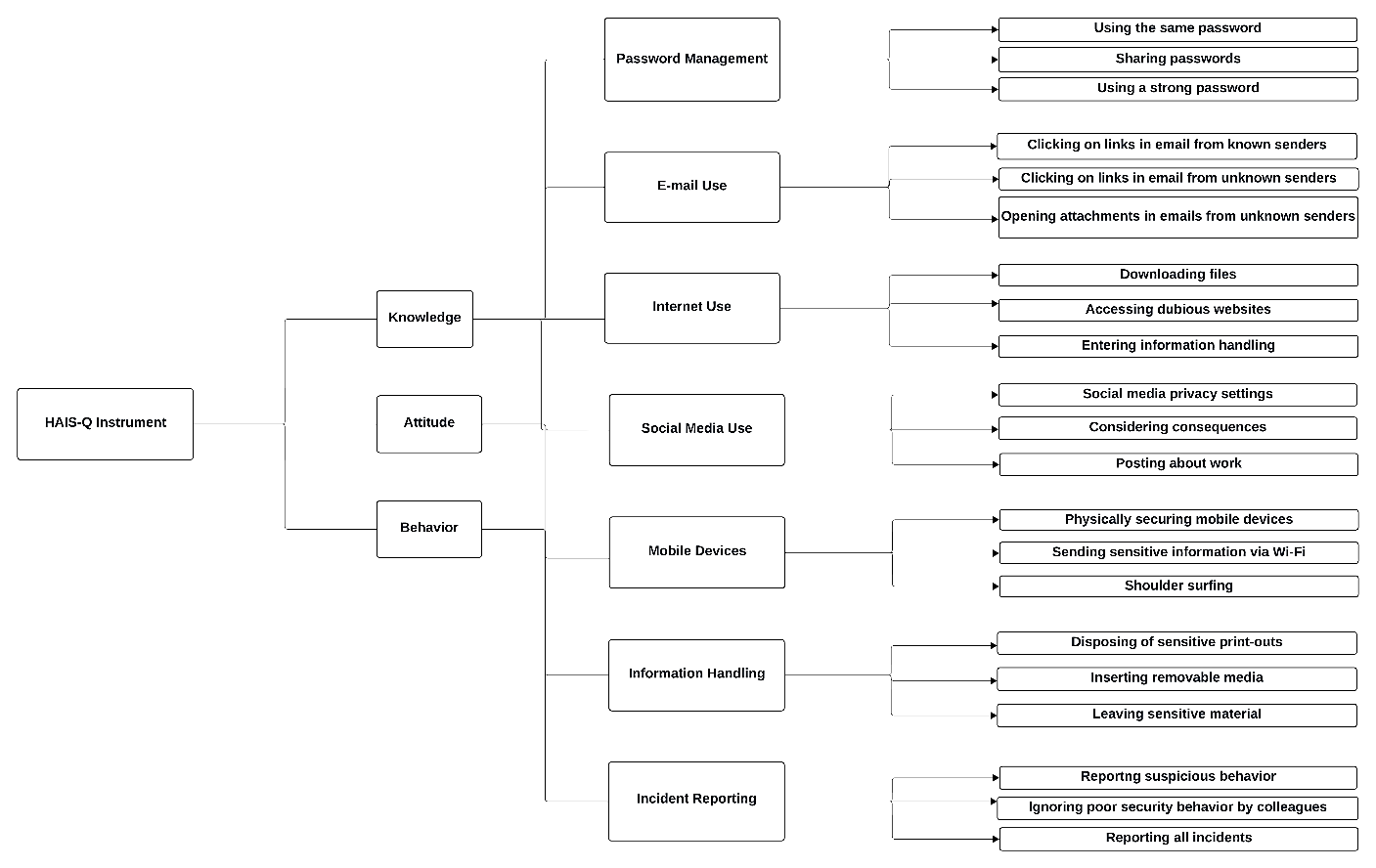
# METHODS

This research used a quantitative descriptive methodology and research methods from (Kruger & Kearney, 2006), who had developed the stages of security awareness assessment. A preliminary selection of the research object was conducted first to start exploring the problems. A media organization in Indonesia that had implemented the ISA program had been chosen as the research objects.

The respondents were chosen based on their roles as IT Infrastructure organizational members in the research objects with a total of 60 people. The IT Infrastructure departments in the research objects will manage hardware, networks, information security and IT support. Additionally, all of IT Infrastructure organizational members have received a security awareness training program. The respondents played a very important role in managing the information technology used by the research objects. In addition, the activities carried out by the respondents are very closely related to internet usage. If there was an error caused by the respondents, it could emerge an information security threat that would give negative feedback for the research objects.

Most of the respondents were men with a total of 58 people who had a percentage of 97%. While the other two respondents were women with a percentage of 3%. The majority of respondents in the study were in the age range of 25-30 years with a total of 25 respondents. There were 16 respondents were in the age range of 31-35 years, eight respondents were in the age range of 36-40 years, six respondents were in the age range of 18-24 years and two respondents were in the age range of over 45 years. This ensured a diverse and representative sample of individuals with varying levels of exposure to security awareness initiatives.

To support the research method, the Human Aspect of Information Security Questionnaire (HAIS-Q) instrument developed by (Parsons et al., 2017) on **FIGURE 1** were used to describe each focus area of knowledge, attitude, and behavior (KAB) dimensions.



**FIGURE 1**. Hierarchy of HAIS-Q Instrument

After describing the methods and population, the assessments stages were conducted as follows:

1. Categorization of ISA Measurement Results:

The categorization was carried out based on the values generated from the calculation process in sub-focus areas, focus areas, and dimensions on **TABLE 1**. The categorization used was as follows:

**TABLE 1**. Assessment Categorization Results

|  |  |  |
| --- | --- | --- |
| Awareness Value | Awareness Category | Action |
| 80% - 100% | Good | Satisfactory – no action required |
| 60% - 79% | Average | Monitor – action potentially required |
| < 59% | Poor | Unsatisfactory – action required |

1. Questionnaire preparation:

The HAIS-Q instrument was used as a questionnaire, and it presented 63 statements. Each statement on the questionnaire had a five-point scale ranging from "Strongly Disagree" to "Strongly Agree". There were several statements that had the symbol "^", which required reverse scoring by changing the point scale of a statement that was carried out on **TABLE 2** and **TABLE 3**.

**TABLE 2**. Unreversed Scoring Value (Without “^”)

|  |  |
| --- | --- |
| Awareness | Description |
| 1 | Strongly Disagree |
| 2 | Disagree |
| 3 | Neutral |
| 4 | Agree |
| 5 | Strongly Agree |

**TABLE 3**. Reverse Scoring Value (With “^”)

|  |  |
| --- | --- |
| Awareness | Description |
| 1 | Strongly Agree |
| 2 | Agree |
| 3 | Neutral |
| 4 | Disagree |
| 5 | Strongly Disagree |

The questionnaire that had been prepared was distributed to the respondents. The distribution period was carried out in March 2024. The distribution of the questionnaire was carried out in the first week of March 2024 by sending an e-mail to the respondents. The e-mail included the URL for filling the form in a Google Form platform along with the instructions for filling out the questionnaire. For 3 weeks, the respondents provided the answers to the questionnaire. After the questionnaire had been filled out, the next stage was analyzing the results of the questionnaire.

1. Data processing:

This stage was the process of analyzing the results of the questionnaire. There were three steps for security awareness scores calculations conducted on this stage.

1. Sub focus area calculations

The first step was calculating the answers of the questionnaire. The researcher summed up the points according to the scales of all statement answers from a sub-focus area. After that, these results were divided by the maximum score of the statement item. The maximum score was obtained by multiplying the number of respondents with the questionnaire scale. The result of that calculation was the respondents’ perception scores from a statement in a sub-focus area. These processes were repeated until all statements in the sub-focus area had been done.

1. Focus area calculations

The next step was calculating the average score of the sub-focus area in a focus area. The result of that calculation was the respondents’ perceptions scores from the focus area in each dimension. The process was repeated until all focus areas of a dimension had been done.

1. Dimension calculation

This step calculated the average score of the focus area in a dimension. The result of that calculation was the respondents’ perceptions scores in a dimension. The process was repeated until all the knowledge, attitude, and behavior dimensions were calculated.

# RESULTS AND DISCUSSION

## ASSESSMENT RESULTS

The calculation result from respondents’ questionnaire firstly was be described based on focus area in the **TABLE 4** below.

**TABLE 4**. Focus Area Calculation Results

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Focus Area | Awareness Value (%) | | | Total Awareness (%) | Awareness Category | Action |
| K | A | B |
| Password Management | 87 | 81 | 84 | 84% | Good | Satisfactory – no action required |
| Email Use | 75 | 78 | 79 | 77% | Average | Monitor – action potentially required |
| Internet Use | 67 | 72 | 75 | 71% | Average | Monitor – action potentially required |
| Social Media Use | 76 | 81 | 80 | 79% | Average | Monitor – action potentially required |
| Mobile Devices | 81 | 81 | 84 | 82% | Good | Satisfactory – no action required |
| Information Handling | 81 | 84 | 86 | 84% | Good | Satisfactory – no action required |
| Incident Reporting | 77 | 78 | 80 | 78% | Average | Monitor – action potentially required |

1. Password Management

Most sub-focus areas had a "Good" assessment result. It indicated that the respondents had a good perception towards those focus areas. Therefore, the research object did not need to be enhanced those sub-focus areas. However, a sub-focus area in the attitude and behavior dimension had an "Average" assessment result. It indicated that the respondents had a sufficient perception towards those focus areas. Hence, the research object was able to enhance those focus areas.

These results could be analyzed to create new information regarding the respondents’ perceptions in the password management focus area. Based on the calculation, these focus areas had a “Good” assessment result, which indicated that the respondents had a good perception. As a result, there was no need for the research object to improve these areas, as they were already good perceived about it.

1. E-mail Use

Most sub-focus areas had a "Good" assessment result. It indicated that the respondents had a good perception towards those sub-focus areas. Therefore, the research object needed to be maintained. However, two sub-focus areas in the knowledge dimension had been assessed as "Average" and one sub-focus area in the attitude and behavior dimension also had an "Average" assessment result. It indicated that the respondents had a sufficient perception towards those focus areas. As a result, the research object was able to enhance those sub-focus areas.

These results could be calculated to create new insights regarding respondents’ perceptions in the e-mail use focus area. These focus areas had an “Average” assessment result, which indicated that the respondents had a sufficient perception in those focus areas. So that the research object is able to enhance those focus areas.

1. Internet Use

There were three sub-focus areas in the attitude and behavior dimension that had a "Good" assessment result. The two sub-focus areas in the behavior dimension also had a "Good" assessment result which presented that the respondents had a good perception towards those sub-focus areas. It could be drawn that the research object did not need to enhance those sub-focus areas. However, the most sub-focus areas in the internet use focus area had an "Average" assessment result. It showed that the respondents had a sufficient perception towards those focus areas which made the research object able to enhance those sub-focus areas.

These could be calculated to draw new information regarding the respondents’ perceptions in the internet use focus area. These focus areas presented an “Average” assessment result, indicating respondents had a sufficient perception. Therefore, the research objects had been able to enhance those focus areas.

1. Social Media Use

The research results showed that most sub-focus areas had a "Good" assessment result. This result indicated that the respondents had a clear understanding towards those sub-focus areas and the research object did not need to enhance those sub-focus areas. However, the two sub-focus areas in the knowledge dimension presented an "Average" assessment result while the other one sub-focus area in the attitude and behavior dimension also had an "Average" assessment result. Both results indicated that the respondents have a sufficient perception towards those focus areas. Hence, the research object was able to enhance those sub-focus areas.

New information regarding respondent perceptions in the social media use focus area could be drawn. The study presented that these focus areas had an “Average” assessment result. By this, the respondents should have had a sufficient perception. Relating to this result, the research object had been able to enhance those focus areas.

1. Mobile Devices

There was a sub-focus area in the attitude and behavior dimension that had a "Good" assessment result. This showed that the respondents had already a good understanding of those sub-focus areas. It noted a statement that the research object was not necessarily enhancing those sub-focus areas. Other than that, the most sub-focus areas had an "Average" assessment result. It also indicated that the respondents had a sufficient understanding which made the research object able to enhance those sub-focus areas.

Consequently, new information regarding the respondents’ perceptions in the mobile devices focus area had been drawn. According to the calculation, these focus areas had a “Good” assessment result. It revealed that the respondents have a good comprehension which obliged the research object to not enhance those focus areas.

1. Information Handling

It had been revealed that the most sub-focus areas had a "Good" assessment result. It pointed out that the respondents had a clear perception towards those sub-focus areas. This drew attention to the fact that the research object did not enhance those sub-focus areas necessarily. However, one sub-focus area in the knowledge dimension had been assessed as "Average". It indicated that the respondents had a sufficient perception towards those sub-focus areas and being able to enhance it.

It created new information regarding the respondents’ perceptions in the information handling focus area. Based on the calculation, these focus areas had a “Good” assessment result, indicating that the respondents had a good perception. As a result, there was no need for the research object to improve these areas, as they were already good perceived about it.

1. Incident reporting

The study presented that there was a sub-focus area in the attitude dimension that had been assessed as "Good" category. Meanwhile, there were two sub-focus areas in the behavior dimension that also had a "Good" assessment result. It showed that the respondents had a good understanding of those sub-focus areas. Hence, the research objects did not necessarily enhance those sub-focus areas. Subsequently, the most sub-focus areas had an "Average" assessment result. It showed that the respondents had a sufficient perception towards those sub-focus areas. Thus, the research object was able to enhance those focus areas.

The results could be used to generate new insights into how the respondents perceived incident reporting focus area. According to the analysis, these focus areas received an "Average" assessment result, suggesting that the respondents had an adequate perception. As a result, the research object is able to enhance those focus areas.

Following the explanation of the sub-focus areas and dimensions, the **TABLE 5** will carried out the assessment results based on the KAB dimensions.

**TABLE 5**. KAB Dimensions Calculation Results

|  |  |  |  |
| --- | --- | --- | --- |
| Dimensions | Awareness Value (%) | Awareness Category | Action |
| Knowledge | 78 | Average | Monitor – action potentially required |
| Attitude | 79 | Average | Monitor – action potentially required |
| Behavior | 81 | Good | Satisfactory – no action required |

The dimensions labeled behavior had received a "Good" assessment, signifying that the respondents held a positive perception of the dimensions. As a result, there was no need for the research object to enhance these dimensions. On the other hand, the dimensions of knowledge and attitude had been assessed as "Average", indicating that the respondents had a sufficient perception of these dimensions. Consequently, the research object could enhance these dimensions.

The information in TABLE 5 could be used to represent the respondents' general perceptions towards these programs. In that case, the result presented the score with "79", which had an "Average" category. The respondents' perceptions of those programs were adequate, indicating that the research object could enhance the security awareness programs focusing on specific areas or the knowledge, attitude, behavior (KAB) dimensions.

## RECCOMMENDATIONS

Following the detailed explanations above, the assessment findings could be utilized to provide suggestions for the research objects. These recommendations aim to improve awareness of information security amongst the respondents. Additionally, it can be implemented in a certain stage by the management of information security research objects.

1. Password management

The attitude dimension could be enhanced by providing suggestions regarding the impact of information security threats when sharing personal organization account passwords with other colleagues. Meanwhile, the enhancement of the behavioral dimension could be done by holding simulation training regarding information security incidents resulting from the same password usage in the organization accounts.

1. E-mail Use

Enhancing the behavioral dimension could be done by holding simulation training in the form of e-mail phishing simulations involving known senders. Then, enhancing the attitude dimension could be carried out by providing suggestions regarding the impact of information security threats that could happen when users did not validate e-mail from known senders. Meanwhile, in enhancing the knowledge dimension, it could be accomplished by providing knowledge about validation activities regarding an e-mail from known and unknown senders.

1. Internet Use

The behavioral dimension could be enhanced by holding simulation training in the form of driving-by download and web phishing attacks. The enhancement of the attitude dimensions could be carried out by providing suggestions regarding the impacts of information security threats that might be happened caused by unfiltered activities when downloading data from the internet, as well as the impact when users give their data on a website. Besides, the enhancement in the knowledge dimension could be done by providing knowledge about filtering data to be downloaded from the internet, accessing a website, and giving any information on a website.

1. Social Media Use

Enhancing the attitude dimension could be accomplished by providing suggestions regarding the impact of information security threat when users did not set privacy rules for their social media accounts. Aside from that, the behavioral dimension could be enhanced by holding simulation training for the privacy settings of social media accounts. Meanwhile, enhancing knowledge dimension could be accomplished by providing knowledge about privacy settings in their social media accounts and the consequences of social media usage in the digital age.

1. Mobile Devices

Enhancing the knowledge dimension could be fulfilled by providing knowledge regarding how to secure mobile devices in public areas, public Wi-Fi networks usage, and shoulder surfing activities. The attitude dimension could be enhanced by providing suggestions regarding the impact of information security threats that could be affected by sending sensitive data using public Wi-Fi networks. Meanwhile, enhancing the behavioral dimension could be accomplished by holding a simulation training regarding sending sensitive data using public Wi-Fi networks.

1. Information Handling

The knowledge dimension could be enhanced by providing knowledge regarding storage mechanisms for physical documents that contained sensitive data.

1. Incident reporting:

In gaining the enhancement of knowledge dimension, it could be done by providing knowledge related to detecting suspicious activities amongst colleagues, paying attention to poor information security behavior amongst colleagues, and reporting any security incidents that might occur in the organization. While enhancing the behavioral dimension could be done by holding a simulation training for detecting any suspicious activities amongst colleagues. The last was enhancing the attitude dimension that could be carried out by providing suggestions regarding the impact of information security threats when poor information security practices were allowed amongst colleagues and ignored an information security incident in the organization.

# CONCLUSIONS

The results of the analysis and discussion of security awareness assessment provided some information that could be used as conclusions in this research. Security awareness assessment results helped research objects to perceive the perceptions amongst their organizational members towards those programs. In general, the organizational members already had sufficient perceptions of the security awareness with a descriptive explanation of their perceptions based on the focus area and the knowledge, attitude, and behavior (KAB) dimensions. According to the focus area assessment results, good perceptions were held by the respondents in some focus areas such as password management, mobile devices and information handling. Meanwhile, the respondents had sufficient perceptions on the areas of e-mail use, internet use, social media use, and incident reporting. Afterwards, the KAB dimensions assessment results and analysis presented that the good perception was held by respondents in the behavior dimension. Meanwhile, the respondents had sufficient perception on the knowledge and attitude dimensions.

By conducting this assessment, the researcher had drawn a conclusion to the research objects for enhancing security awareness program amongst the respondents. This study formed a verification stage for the research object in the security awareness program. Additionally, this study also contributed to other organizations that did not have an assessments method of the security awareness program. Therefore, the organization might have a broader perspective to enhance the performance of human factors at information security and security awareness program. The limitation of this study was the subjectivity of the respondents when filling out questionnaires. Therefore, further research can be considered cyber fatigue factors amongst the organizational members and put another focus area that has relevance with emerging threats and organizational needs.

# Acknowledgments

I would like to express my sincere gratitude to Mr. Nilo Legowo for the invaluable mentorship and guidance throughout this study. His expertise in the information security field was a great line in shaping this study direction. Additionally, I would like to express gratitude to the Information System Management Department, Bina Nusantara University. I thank all the respondents for their willingness to participate in this study and for sharing their insights. Their contributions were essential to the success of this study.

# References

1. M. Zammani, R. Razali, and D. Singh, "Organisational information security management maturity model," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 9, 2021.
2. X. Liu *et al.*, "Cyber security threats: A never-ending challenge for e-commerce," *Frontiers in psychology,* vol. 13, p. 927398, 2022.
3. M. Zammani and R. Razali, "An empirical study of information security management success factors," *International Journal on Advanced Science Engineering Information Technology,* vol. 6, no. 6, pp. 904-913, 2016.
4. N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *computers & security,* vol. 56, pp. 70-82, 2016.
5. R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity,* vol. 3, pp. 1-18, 2020.
6. M. Zammani, R. Razali, and D. Singh, "Factors contributing to the success of information security management implementation," *International Journal of Advanced Computer Science and Applications,* vol. 10, no. 11, 2019.
7. M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *computers & security,* vol. 73, pp. 345-358, 2018.
8. L. Alzahrani and K. P. Seth, "The impact of organizational practices on the information security management performance," *Information,* vol. 12, no. 10, p. 398, 2021.
9. K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & security,* vol. 106, p. 102267, 2021.
10. M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: a systematic mapping study," *Arabian Journal for Science and Engineering,* vol. 45, pp. 3171-3189, 2020.
11. S. Hina and P. D. D. Dominic, "Information security policies’ compliance: a perspective for higher education institutions," *Journal of Computer Information Systems,* vol. 60, no. 3, pp. 201-211, 2020.
12. M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems,* vol. 62, no. 1, pp. 82-97, 2022.
13. R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance," *Applied Sciences,* vol. 11, no. 8, p. 3383, 2021.
14. M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in *International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 352-358: IEEE.
15. R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon,* vol. 9, no. 3, p. e14234, 2023.
16. Š. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," *Information & Computer Security,* vol. 29, no. 1, pp. 133-158, 2021.
17. K. Kannelønning and S. K. Katsikas, "A systematic literature review of how cybersecurity-related behavior has been assessed," *Information & Computer Security,* vol. 31, no. 4, pp. 463-477, 2023.
18. L. Yin, Y. Sun, Z. Wang, Y. Guo, F. Li, and B. Fang, "Security measurement for unknown threats based on attack preferences," *Security and Communication Networks,* vol. 2018, no. 1, p. 7412627, 2018.