ICEBIT
The 4th International Conference On Economics , Business and Information Technology
June 10, 2023 pp. 861-866

Evaluating Individual Involvement in Shaping Information Security Culture

Nur Andita Prasetyo
Institut Teknologi dan Sains Mandala
Jl. Sumatra No.118-120, Jember
+62 823-2920-1769
nurandita.prasetyo69@itsm.ac.id

Mas'ud Hermansyah
Institut Teknologi dan Sains Mandala
Jl. Sumatra No.118-120, Jember
+62 813-3646-6463
masudhermansyah@itsm.ac.id

Iqbal Sabilirrasyad
Institut Teknologi dan Sains Mandala
Jl. Sumatra No.118-120, Jember
+62 851-7124-3269
iqbal@itsm.ac.id

Fauzan Azim
Institut Teknologi dan Sains Mandala
Jl. Sumatra No.118-120, Jember
+62 823-8558-4973
fauzan@itsm.ac.id

ABSTRACT

In the increasingly advanced digital era, information security has become a crucial aspect for various organizations worldwide. In facing these challenges, organizations rely not only on sophisticated security technologies but also on active participation and involvement of individuals in shaping a strong information security culture. Information security culture encompasses the attitudes, values, and behaviors of individuals when it comes to addressing information security risks. This research aims to evaluate the individual involvement in shaping the information security culture within an organization. The study will involve measuring the level of individual awareness of information security, individual knowledge of information security, compliance with security policies and procedures, as well as individual behaviors in maintaining information security. Data collection will be done using a questionnaire that has been tested for validity and reliability. Awareness has an average total score of 13.20833333 and an average dimension score of 4.40277778. Meanwhile, knowledge has the same value as compliance and behavior, with an average total score of 13.27083333 and an average dimension score of 4.42361111. The results of this research reveal that the research subject has the lowest awareness value compared to other dimensions, while knowledge, compliance, and behavior have the same values. Overall, the research subject exhibits a relatively good information security culture, although it is not perfect.

Keywords : information security culture, information security awareness, behavior analysis, individual involvement, quantitative measurement evaluation

1. INTRODUCTION

In the increasingly advanced digital era, information security has become a crucial aspect for various organizations worldwide. Threats to information security continue to evolve, both from complex cyber-attacks and potential internal threats. In facing these challenges, organizations rely not only on sophisticated security technologies but also on active participation and involvement of individuals in shaping a robust information security culture (Nur Andita Prasetyo, 2022).

Information security culture encompasses the attitudes, values, and behaviors of individuals when it comes to addressing information security risks. This involves individuals' understanding of the importance of information security, their level of compliance with security policies and procedures, and their active participation in efforts to maintain information security. Evaluating individual involvement in shaping information security culture is an important step in understanding the extent to which individuals contribute to maintaining information security in the workplace (Adéle da Veiga, 2020).

The significance of individual involvement in information security cannot be ignored. Studies have shown that successful cyber-attacks often involve human factors, such as carelessness, ignorance, or violations of security policies. Therefore, individual awareness and engagement in implementing good security practices are essential to mitigate information security risks (Akhyari Nasir, 2019).

Evaluating individual involvement in shaping information security culture involves measuring the extent to which individuals understand the importance of information security, their level of compliance with security policies and procedures, and their active participation in security efforts. By conducting this evaluation, organizations can identify strengths and weaknesses in the existing information security culture and determine necessary improvement measures. This research aims to evaluate individual involvement in shaping information security culture within an organization. The study will involve measuring the level of individual awareness of information security, individual knowledge of information security, compliance with security policies and procedures, as well as individual behaviors in maintaining information security (Akhyari Nasir, 2017).

2. RESEARCH METHOD

This study utilizes a survey research design with a questionnaire as the data collection instrument. The questionnaire will be distributed to respondents consisting of employees of Diskominfo Jember:

2.1 Questionnaire Development

The questionnaire will consist of several sections that include:

a. Information Security Awareness: This section will include questions regarding awareness of threats and issues related to information security (WookJoon Sung, 2017). The statements are:
    a. I am aware of my role and responsibility in information security.
    b. I am aware of the risks of not following information security policies.
    c. I am aware of the information security policies.

b. Knowledge of Information Security: This section will measure respondents' knowledge about the importance of employee commitment to protecting information (Puspita Kencana Sari, 2021). The statements are:
    a. I understand the importance of protecting personal, sensitive, and confidential information.
    b. I understand the negative consequences of information security issues.
    c. I am aware of the authority of Information Security within the organization

c. Compliance with Security Policies and Procedures: This section will evaluate the level of respondents' compliance with existing security policies and procedures in the organization, such as password policies, software usage policies, or data access policies (Puspita Kencana Sari, 2021). The statements are:
    a. Leaders communicate clear directions on protecting information to employees or third parties.
    b. I follow the established information security procedures/policies by the organization.
    c. I am aware of my role in information security but do not fully adhere to current practices

d. Behavior in Information Security Efforts: This section will measure the level of active participation by respondents in maintaining information security (Puspita Kencana Sari, 2021). The statements are:
    a. I do not leave sensitive/secret information in insecure places.
    b. I regularly check documents for malware infections.
    c. I consider the negative consequences of their work before posting anything on social networking sites

e. Rating Scale: Each section will use a Likert rating scale to measure the level of understanding, compliance, and active participation of respondents regarding information security. The rating scale can range from 1 to 5, with 1 indicating a low level and 5 indicating a high level.

2.2 Data Collection

The questionnaire will be directly distributed to the respondents, in this case, the employees of Diskominfo Jember. The data collection period will be determined based on the research needs.

2.3 Data Analysis

The data collected through the questionnaire will be analyzed using relevant statistical techniques, including reliability and validity tests.

2.4 Validity Test

Table 1. Awareness Validity Test

Correlations

		Awareness1	Awareness2	Awareness3	Awareness
Awareness1	Pearson Correlation	1	.454**	.075	.759**
	Sig. (2-tailed)		.001	.615	.000
	N	48	48	48	48
Awareness2	Pearson Correlation	.454**	1	.416**	.833**
	Sig. (2-tailed)	.001		.003	.000
	N	48	48	48	48
Awareness3	Pearson Correlation	.075	.416**	1	.609**
	Sig. (2-tailed)	.615	.003		.000
	N	48	48	48	48

Awareness	Pearson Correlation	.759**	.833**	.609**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the "Correlations" output above, it is known that the Sig. value (2-tailed) for the relationship or correlation between Awareness1 and Awareness is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.759 > 0.368. Therefore, it can be concluded that Awareness1 is valid. Similarly, the correlation between Awareness2 and Awareness is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.833 > 0.368, indicating that Awareness2 is valid. Furthermore, the correlation between Awareness3 and Awareness is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.609 > 0.368, indicating that Awareness3 is valid. Since the items Awareness1, Awareness2, and Awareness3 are deemed valid, these items can be considered as accurate data collection tools in a research study.

Table 2. Knowledge Validity Test

Correlations

		Knowledge1	Knowledge2	Knowledge3	Knowledge
Knowledge1	Pearson Correlation	1	.484**	.114	.786**
	Sig. (2-tailed)		.000	.439	.000
	N	48	48	48	48
Knowledge2	Pearson Correlation	.484**	1	.375**	.823**
	Sig. (2-tailed)	.000		.009	.000
	N	48	48	48	48
Knowledge3	Pearson Correlation	.114	.375**	1	.602**
	Sig. (2-tailed)	.439	.009		.000
	N	48	48	48	48
Knowledge	Pearson Correlation	.786**	.823**	.602**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the above "Correlations" output, it is observed that the Sig. value (2-tailed) for the relationship or correlation between Knowledge1 and Knowledge is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.786 > 0.368. Hence, it can be concluded that Knowledge1 is considered valid. Similarly, the correlation between Knowledge2 and Knowledge is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.823 > 0.368, indicating the validity of Knowledge2. Furthermore, for the correlation between Knowledge3 and Knowledge, the Sig. value is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.602 > 0.368. Consequently, it can be concluded that Knowledge3 is valid. As Knowledge1, Knowledge2, and Knowledge3 are all declared valid, these items can be utilized as accurate data collection tools in a research study.

Table 3. Compliance Validity Test

Correlations

		Compliance1	Compliance2	Compliance3	Compliance
Compliance1	Pearson Correlation	1	.453**	.064	.741**
	Sig. (2-tailed)		.001	.666	.000
	N	48	48	48	48
Compliance2	Pearson Correlation	.453**	1	.511**	.859**
	Sig. (2-tailed)	.001		.000	.000
	N	48	48	48	48

Compliance3	Pearson Correlation	.064	.511**	1	.638**
	Sig. (2-tailed)	.666	.000		.000
	N	48	48	48	48
Compliance	Pearson Correlation	.741**	.859**	.638**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the above "Correlations" output, it is evident that the Sig. value (2-tailed) for the relationship or correlation between Compliance1 and Compliance is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.741 > 0.368. Consequently, it can be concluded that Compliance1 is deemed valid. Similarly, the correlation between Compliance2 and Compliance is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.859 > 0.368, indicating the validity of Compliance2. Furthermore, for the correlation between Compliance3 and Compliance, the Sig. value is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.638 > 0.368. Thus, it can be inferred that Compliance3 is valid. As Compliance1, Compliance2, and Compliance3 are all confirmed to be valid, these questionnaire items can be employed as accurate data collection tools in a research study.

Table 4. Behavior Validity Test

Correlations

		Behavior1	Behavior2	Behavior3	Behavior
Behavior1	Pearson Correlation	1	.452**	.009	.741**
	Sig. (2-tailed)		.001	.952	.000
	N	48	48	48	48
Behavior2	Pearson Correlation	.452**	1	.445**	.850**
	Sig. (2-tailed)	.001		.002	.000
	N	48	48	48	48
Behavior3	Pearson Correlation	.009	.445**	1	.590**
	Sig. (2-tailed)	.952	.002		.000
	N	48	48	48	48
Behavior	Pearson Correlation	.741**	.850**	.590**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	48	48	48	48

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the above "Correlations" output, it is observed that the Sig. value (2-tailed) for the relationship or correlation between Behavior1 and Behavior is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.741 > 0.368. Hence, it can be concluded that Behavior1 is valid. Similarly, the correlation between Behavior2 and Behavior is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.850 > 0.368, indicating the validity of Behavior2. Furthermore, for the correlation between Behavior3 and Behavior, the Sig. value is 0.000 < 0.05, and the Pearson Correlation is positive with a value of 0.590 > 0.368. Therefore, it can be inferred that Behavior3 is valid. Since Behavior1, Behavior2, and Behavior3 are deemed valid, these questionnaire items can serve as accurate data collection tools in a research study.

2.5 Reliable Test

Table 5. Case Processing Summary

Case Processing Summary

		N	%
Cases	Valid	48	100.0
	Excluded[a]	0	.0

Total	48	100.0

a. Listwise deletion based on all variables in the procedure.

The table above provides information on the sample size or respondents (N) analyzed in the SPSS program, which is a total of 48 individuals. Since there is no missing data (meaning all respondent answers are filled), the valid count is 100%.

Table 6. ReliabilityTest

Reliability Statistics

Cronbach's Alpha	N of Items
.883	16

From the table above, it is known that there are N of Items (number of items or questionnaire items) with a total of 12 items and a Cronbach's Alpha value of 0.883. Since the Cronbach's Alpha value is 0.883 > 0.60, it can be concluded that all 12 items or statements in the questionnaire are reliable or consistent.

Using the questionnaire research method, this study is expected to provide a deeper understanding of individual involvement in shaping information security culture. With a better understanding, organizations can take necessary steps to improve information security culture and reduce potential information security risks.

3. RESULT AND DISSCUSION

The following is a description of the results of the study containing the results of the promotion decision analysis using the Simple Additive Weight (SAW) method.

3.1 Results

Table 7. Result

Dimensi	Rata-rata Total	Rata-rata dimensi
Kesadaran	13.20833333	4.40277778
Pengetahuan	13.27083333	4.42361111
Kepatuhan	13.27083333	4.42361111
Behaviour	13.27083333	4.42361111

Source: data collection

The table above shows the total average and dimension average values for each dimension from individuals' perspectives on organizational security culture, namely awareness, knowledge, compliance, and behavior. Awareness has a total average of 13.20833333 and a dimension average of 4.40277778. On the other hand, knowledge has the same value as compliance, and behavior has a total average of 13.27083333 and a dimension average of 4.42361111.

3.2 Discussion

A strong information security culture is a crucial factor in protecting organizations from various information security threats. One key element in shaping a strong information security culture is individual involvement. Evaluating individual involvement in shaping information security culture is an important step in understanding the extent to which individuals contribute to maintaining information security in the workplace (Alaa Tolah, 2021).

Through the evaluation of individual involvement, organizations can identify the level of individuals' understanding of information security. Individual understanding includes knowledge of the potential risks and threats to information security, as well as the practices and policies that need to be followed. This evaluation can help organizations determine whether individuals have received adequate training and education on information security. Additionally, individual understanding can also encompass awareness of the importance of information security in carrying out daily tasks (Aleksandr Ključnikov, 2019).

Furthermore, the evaluation of individual involvement can also assess the level of individuals' compliance with existing security policies and procedures. The success of information security policies relies not only on sound policies but also on the level of individual compliance in implementing them. This evaluation can help organizations identify any weaknesses in the implementation of information security policies and determine if additional efforts are needed to enhance individual compliance (Alifiani Kurniati, 2020).

In addition to understanding and compliance, the evaluation of individual involvement also assesses individuals' active participation in maintaining information security. Active participation includes individual behaviors in

implementing information security policies. This evaluation can help organizations assess the level of individuals' proactive engagement in safeguarding information security (Anna Georgiadou, 2020).

When conducting evaluations of individual involvement, research methods that utilize questionnaires can be effective tools. Questionnaires can summarize relevant questions regarding individual awareness, compliance, knowledge, and active behaviors related to information security. By using Likert rating scales, the data obtained from questionnaires can be analyzed to depict the overall level of individual involvement (Valuch, 2017).

Through the evaluation of individual involvement in shaping information security culture, organizations can gain valuable insights to identify strengths and weaknesses in the existing information security culture. The findings of this evaluation can serve as a basis for developing more effective strategies to enhance individual involvement in shaping information security culture (WookJoon Sung, 2017).

4. CONCLUTION

The evaluation of individual involvement in shaping information security culture is an important step in increasing individual awareness and engagement in safeguarding information security in the workplace. By using appropriate research methods, organizations can gain valuable insights to identify areas that need improvement and develop more effective strategies in shaping a strong information security culture. By actively involving individuals, organizations can create a security-conscious work environment and protect their information assets from security threats. The results of this study reveal that the research subject has the lowest awareness score among the other dimensions, while knowledge, compliance, and behavior have the same score. Overall, the research subject has a relatively good information security culture, although it is not perfect.

REFERENCES

Adéle da Veiga, L. V. (2020). Defining organisational information security culture – Perspectives from academia and industry. *Computers & Security*.

Akhyari Nasir, R. A. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. *ICISDM*.

Akhyari Nasir, R. A. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*.

Alaa Tolah, S. M. (2021). An Empirical Analysis of the Information Security Culture Key Factors Framework. *Computers & Security*.

Aleksandr Ključnikov, L. M. (2019). Information Security Management in SMEs: Factors of Success. *Journal of Entrepreneurship and Sustainability Issues*, 2081-2094.

Alifiani Kurniati, L. E. (2020). Manajemen Risiko Teknologi Informasi pada e-Government: Ulasan Literatur Sistematis (Information Technology Risk Management on e-Government: Systematic Literature Review). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, 207-222.

Anna Georgiadou, S. M. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*.

Nur Andita Prasetyo, B. S. (2022). Kajian Dimensi Budaya Keamanan Informasi dalam Berbagai Organisasi. *Jurnal Teknologi Rekayasa, 7*, 73-82.

Puspita Kencana Sari, A. P. (2021). Information security cultural differences among health care facilities in Indonesia. *Heliyon*.

Valuch, J. (2017). Cyber Attacks, Information Attacks, And Postmodern Warfare. *Balt. J. Law Polit.*, 63–89.

WookJoon Sung, S. K. (2017). An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness. *Proceedings of dg.o'17.* New York.