ICEBIT
The 5th International Conference On Economics , Business and Information Technology
E-ISSN 3025-4892
August 24, 2024 pp. 445-452

Comparison of Information Security Cultures: Evaluation from the Perspective of Individuals in Organizations

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

M. Faiz Firdausi
Institut Teknologi dan Sains Mandala
Jl. Sumatra No.118-120, Jember
+62 823-8558-4973
faizfirdausi@itsm.ac.id

ABSTRACT

This research evaluates comparative information security cultures across organizations, focusing on individual perspectives regarding awareness, knowledge, compliance, and behavior. This research involved three types of organizations: Organization A, which operates entirely in the IT sector; Organization B, a non-IT organization that uses IT in its operations; and Organization C, also a non-IT organization but using IT in a limited capacity. The results showed that Organization A obtained the highest scores in all categories measured—awareness (4.4), knowledge (4.42), compliance (4.42), and behavior (4.42)—indicating understanding and implementation of IT practices excellent performance and a strong commitment to information security standards. In contrast, Organization B showed lower mean scores—awareness (3.75), knowledge (3.74), compliance (3.71), and behavior (3.79)—indicating less than optimal IT integration and implementation despite the technology used. Organization C, which uses IT to a limited extent, shows results that fall between those of Organizations A and B—awareness (3.97), knowledge (4), compliance (3.92), and behavior (3.96)—indicating good knowledge. good but faces challenges in full integration and practice. These findings confirm the relationship between an organization's focus on IT and the effectiveness of information security practices. To improve an information security culture, organizations need to focus on improving training and education, strengthening policies and procedures, investing in IT resources, increasing technology integration, and building an organizational culture that supports information security. These steps are important to address existing deficiencies, increase security effectiveness, and better protect data and information.

Keywords : information security culture, individual involvement, quantitative measurement evaluation

1. INTRODUCTION

In an increasingly advanced digital era, information security has become a very important issue for organizations in various sectors. Organizations must protect their data and information from ever-evolving security threats, such as cyberattacks, data leaks, and misuse of information. (Nur Andita Prasetyo, 2022). To achieve optimal levels of security, organizations need to develop a strong information security culture. Information security culture involves understanding, awareness, compliance, and participation of all members of the organization in maintaining information security.

However, information security culture is not static and can differ from one organization to another. Each organization has unique characteristics, policies and culture.(Akhyari Nasir, 2019). Therefore, it is important to understand the comparison of information security culture in various organizations to identify differences, similarities, and factors that influence information security culture. In this context, evaluating information security culture from an individual's perspective becomes very relevant. Individuals within an organization have a key role in shaping an information security culture. (Alaa Tolah, 2021). They are users, managers, or holders of information who are responsible for protecting and maintaining the confidentiality of organizational data. (Aleksandr Ključnikov, 2019). The individual perspective in evaluating information security culture provides insight into an individual's level of understanding, awareness, behavior and participation in maintaining information security.

In this article, we will evaluate from an individual perspective the information security culture in various organizations. Our main goal is to carry out a comparison between information security cultures in different organizations and identify the factors that influence them. In this context, we will explore questions such as: How do information security cultures differ in different organizations? How do individuals' understanding, awareness, and participation in maintaining information security vary among these organizations? What factors influence information security culture from the perspective of individuals in an organization? To achieve this goal, we will use an evaluative approach involving appropriate research methods, such as questionnaires or interviews, to collect data from individuals in various organizations. The data collected will be analyzed comparatively to identify differences and similarities in information security culture. Additionally, we will engage in a review of relevant literature to substantiate our findings and support the analysis conducted.

2. RESEARCH METHOD

The research method used in this study is the questionnaire method. This method is used to conduct a comparative evaluation of information security culture from the perspective of individuals in various organizations. (Alifiani Kurniati, 2020). First, the researcher identified a specific research objective, namely to compare information security culture from an individual perspective in several organizations. The research questions to be answered are differences in understanding, awareness, behavior and individual participation in maintaining information security between these organizations. The questionnaire will consist of several sections that include:

a. Awareness of Information Security: This section will assess how aware respondents are of threats and issues concerning information security (WookJoon Sung, 2017). The items are:
    a. I am aware of my responsibilities regarding information security.
    b. I understand the risks associated with not adhering to information security policies.
    c. I am knowledgeable about the information security policies in place.
b. Knowledge of Information Security: This section will evaluate the respondents' understanding of the significance of employee commitment in safeguarding information (Puspita Kencana Sari, 2021). The items are:
    a. I recognize the importance of protecting personal, sensitive, and confidential information.
    b. I understand the adverse effects of information security issues.
    c. I am aware of the role and authority of Information Security within the organization.
c. Compliance with Security Policies and Procedures: This section will assess how well respondents comply with the organization's security policies and procedures, such as those related to passwords, software use, or data access (Puspita Kencana Sari, 2021). The items are:
    a. Leaders provide clear instructions on information protection to employees or external parties.
    b. I adhere to the organization's information security procedures/policies.
    c. I am aware of my role in information security, though I do not fully follow current practices.
d. Behavior in Information Security Practices: This section will gauge the level of proactive involvement by respondents in maintaining information security (Puspita Kencana Sari, 2021). The items are:
    a. I do not leave sensitive or confidential information in unsecured locations.
    b. I routinely check documents for malware.
    c. I consider the potential negative impacts of my actions before sharing content on social media.
e. Rating Scale: Each section will use a Likert scale to assess the degree of understanding, compliance, and engagement in information security among respondents. The scale ranges from 1 to 5, where 1 represents a low level and 5 represents a high level.

Apart from that, open questions are also included which provide an opportunity for respondents to provide their responses or opinions in more detail. After that, the questionnaire went through a validation process to ensure its reliability. Content validity is carried out to ensure that the questions in the questionnaire cover relevant and important aspects of information security culture. Construct validity is carried out to ensure that the questionnaire effectively measures the variables you want to study.

After validation, the researcher determines the research samples that will be included in this study. The target population of the study was individuals working in different organizations. Sampling was carried out using random sampling techniques or stratified sampling to ensure sample representativeness. Questionnaires are sent to randomly selected respondents or via appropriate communication channels, such as email or online survey platforms. Clear instructions were given to respondents on how to complete the questionnaire and time limits for completing it. After data collection is complete, data analysis is carried out to answer the research questions. Data from the questionnaire is analyzed using appropriate statistical methods, such as descriptive analysis to describe sample characteristics and questionnaire results, as well as comparative analysis to compare data between different organizations. Findings from data analysis are interpreted based on relevant literature.

The research results are then compiled in a structured and systematic research report. Research reports include a description of the research methodology, main findings, data analysis, and interpretation of the results. The implications of the findings for the culture of information security in organizations are discussed in the discussion. The implications of the findings are debated and analyzed in the context of the needs and challenges faced by organizations related to information security. In addition, the report also provides suggestions for improvement or further development in terms of information security culture. In conducting this research, research ethical considerations are very important. The privacy and confidentiality of respondent data must be maintained by ensuring that this research complies with research ethical standards. Voluntary consent from respondents must be obtained before they participate in research, and they must understand the purpose of the research and the use of their data.

The research method using questionnaires provides an effective approach in collecting data from the perspective of individuals in the organization.(Alan Dennis, 2019). By using this method, researchers can gain deep insight into

the comparison of information security cultures in several organizations. This research provides a better understanding of the factors that influence information security culture and makes an important contribution to the development of more effective information security strategies in the future.

Thus, the research method using a questionnaire is the right approach to carry out a comparative evaluation of information security culture from the perspective of individuals in the organization. In this research, questionnaires were used to collect relevant and significant data from respondents representing various organizations. The results of this research can provide valuable information for organizations in developing and improving their information security culture.

2.1 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).

According to the "Correlations" output above, the significance value (2-tailed) for the correlation between Awareness1 and Awareness is 0.000, which is less than 0.05, and the Pearson Correlation is positive at 0.759, which is greater than 0.368. This indicates that Awareness1 is valid. Similarly, the correlation between Awareness2 and Awareness is also 0.000, less than 0.05, and the Pearson Correlation is positive at 0.833, exceeding 0.368, demonstrating that Awareness2 is valid. Additionally, the correlation between Awareness3 and Awareness is 0.000, below 0.05, with a positive Pearson Correlation of 0.609, which is greater than 0.368, confirming that Awareness3 is valid. Since Awareness1, Awareness2, and Awareness3 are all validated, these items are considered reliable for data collection in the 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).

According to the "Correlations" output above, the significance value (2-tailed) for the correlation between Knowledge1 and Knowledge is 0.000, which is less than 0.05, and the Pearson Correlation is positive at 0.786, exceeding 0.368. This indicates that Knowledge1 is valid. Similarly, the correlation between Knowledge2 and Knowledge is 0.000, which is less than 0.05, and the Pearson Correlation is positive at 0.823, greater than 0.368, confirming that Knowledge2 is valid. Additionally, the correlation between Knowledge3 and Knowledge has a significance value of 0.000, below 0.05, and a positive Pearson Correlation of 0.602, which is higher than 0.368, verifying the validity of Knowledge3. Since Knowledge1, Knowledge2, and Knowledge3 are all validated, these items can be considered reliable for data collection in the 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).

From the "Correlations" output above, it is clear that the significance value (2-tailed) for the correlation between Compliance1 and Compliance is 0.000, which is less than 0.05, and the Pearson Correlation is positive at 0.741, which exceeds 0.368. This confirms that Compliance1 is valid. Similarly, the correlation between Compliance2 and Compliance has a significance value of 0.000, below 0.05, and a positive Pearson Correlation of 0.859, greater than 0.368, validating Compliance2. Additionally, the correlation between Compliance3 and Compliance shows a significance value of 0.000, under 0.05, with a positive Pearson Correlation of 0.638, surpassing 0.368, confirming the validity of Compliance3. Since Compliance1, Compliance2, and Compliance3 are all validated, these items can be used as reliable tools for data collection 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).

According to the "Correlations" output above, the significance value (2-tailed) for the correlation between Behavior1 and Behavior is 0.000, which is less than 0.05, and the Pearson Correlation is positive at 0.741, exceeding 0.368. This confirms that Behavior1 is valid. Similarly, the correlation between Behavior2 and Behavior has a significance value of 0.000, under 0.05, and a positive Pearson Correlation of 0.850, greater than 0.368, indicating that Behavior2 is valid. Additionally, the correlation between Behavior3 and Behavior shows a significance value of 0.000, below 0.05, with a positive Pearson Correlation of 0.590, which is higher than 0.368, demonstrating the validity of Behavior3. Since Behavior1, Behavior2, and Behavior3 are all validated, these items can be used as reliable data collection tools in a research study.

2.2 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 shows that the sample size or number of respondents (N) analyzed using the SPSS program is 48 individuals. As there are no missing data (indicating that all responses are complete), the valid count is 100%.

Table 6. ReliabilityTest

Reliability Statistics

Cronbach's Alpha	N of Items
.883	16

The table above indicates that there are 12 items in the questionnaire with a Cronbach's Alpha value of 0.883. Since this value exceeds 0.60, it demonstrates that all 12 items are reliable and consistent.

By employing this questionnaire-based research method, the study aims to enhance the understanding of individual contributions to developing an information security culture. With these insights, organizations can implement strategies to strengthen their information security culture and mitigate potential security risks.

3. RESULT AND DISSCUSION

In this research, a table is presented that groups organizations based on their types and characteristics. This table divides organizations into three main categories: Organization A, which operates entirely in the IT sector; Organization B, a non-IT organization that uses IT in its operations; and Organization C, a non-IT organization with limited IT use. These groupings are important for understanding how differences in focus and use of technology can influence the results of questionnaires regarding information security culture.

Table 1. Characteristics of Respondents according to organization

Organization	Characteristics of IT use
Organization A	IT
Organization B	Non IT, using IT
Organization C	Non-IT, limited use of IT

After presenting the organizational breakdown, the next table presents the results of the questionnaire measuring four main categories: awareness, knowledge, compliance, and information security-related behavior. The results of this table provide details about the scores obtained from each category for Organizations A, B, and C. By comparing the scores obtained from the three types of organizations, we can evaluate how the characteristics of each organization influence the level of understanding and implementation of security practices information.

3.1 Results

Table 2. Questionnaire Results

Organization	Awareness	Knowledge	Compliance	Behavior
Organization A	4.4	4.42	4.42	4.42
Organization B	3.75	3.74	3.71	3.79
Organization C	3.97	4	3.92	3.96

The research results show clear differences in the level of awareness, knowledge, compliance and behavior between the three organizations with different characteristics. Organization A, which is an IT organization, recorded the highest scores in all categories, with average awareness, knowledge, compliance and behavior scores of 4.4, 4.42, 4.42 and 4.42 respectively. This reflects an excellent level of understanding and application of IT, in line with their primary focus on technology. In contrast, Organization B, which is a non-IT organization but uses IT in its operations, has an average score of awareness, knowledge, compliance, and behavior of 3.75, 3.74, 3.71, and 3.79 respectively. . This value shows that although IT is used in their processes, the level of understanding and application of IT is still below average. Organization C, also a non-IT organization that makes limited use of IT, showed results that were in the middle, with average scores for awareness of 3.97, knowledge of 4, compliance of 3.92, and behavior of 3.96. This shows that although Organization C implements IT on a limited scale, they have good knowledge but still need to improve awareness and compliance aspects of IT use.

3.2 Discussion

The results of a comparative evaluation of information security culture from the perspective of individuals in various organizations provide important insights into how individuals view and participate in efforts to maintain information security. This discussion will outline the main findings of the research, as well as explore the implications and suggestions that can help organizations develop a more effective information security culture.

The results showed that Organization A, which operates entirely in IT, recorded the highest scores in all categories measured—awareness (4.4), knowledge (4.42), compliance (4.42), and behavior (4.42). This is in line with expectations, given that Organization A has a primary focus on technology. This high score reflects excellent understanding and application of IT, as well as consistent commitment and compliance with technology standards. These organizations likely have comprehensive training, adequate resources, and a culture that supports optimal use of technology.

In contrast, Organization B, which is a non-IT organization but integrates IT in its operations, showed lower mean scores—awareness (3.75), knowledge (3.74), compliance (3.71), and behavior (3.79). These results indicate that even though IT is used, the understanding and application of technology in Organization B is still less than optimal. This may be due to a lack of reliance on IT or a lack of adequate training and resources. Lower awareness and compliance may reflect limitations in IT integration and the need for improvements in technology education and training.

Organization C, which is also a non-IT organization but makes limited use of IT, showed scores that were between Organizations A and B—awareness (3.97), knowledge (4), compliance (3.92), and behavior (3.96). This suggests that although Organization C has good knowledge of IT, limited use of technology may hinder the implementation of best practices. Awareness and compliance that still need to be improved indicate challenges in integrating technology into operational processes. Organization C may face obstacles in optimizing the use of technology or in implementing good IT practices.

Overall, these findings indicate that the level of understanding and application of IT is directly proportional to the level of focus and commitment to technology possessed by each organization. Organizations that focus on IT (Organization A) show the best results, while non-IT organizations with limited use of IT (Organization C) and those that use IT generally (Organization B) show variations in scores that reflect the degree of integration and application

of IT in their activities . These findings emphasize the importance of ongoing technology education and adequate support to improve IT-related awareness, knowledge, compliance, and behavior, especially for non-IT organizations that depend on technology for their operations.

Some suggestions that can be given to organizations in improving their information security culture based on the findings of this research are:

1. Increased Training and Education: Organizations, especially non-IT ones, must implement comprehensive training and education programs to increase awareness and knowledge of information security. Regular and updated training can help staff understand risks and best practices in protecting sensitive data and information. (Anna Georgiadou, 2020).
2. Strengthening Policies and Procedures: To improve compliance, organizations need to develop and implement information security policies that are clear and easy to understand. Strict procedures must be followed and monitored regularly to ensure that all members of the organization comply with established security standards. (Choe, 2019).
3. Investment in IT Resources: Non-IT organizations that use IT in their operations should consider investing in better technology infrastructure and IT resources. Procurement of the right software and hardware can support more effective information security management. (Ehab Al-Shaer, 2019)
4. Increased IT Integration: Organizations that use IT in a limited way need to reassess how technology is integrated into their operational processes. Expanding the use of IT and integrating it more deeply into various operational aspects can increase the effectiveness and efficiency of information security. (Gallaugher, 2020)
5. Organizational Culture and Awareness: Building an organizational culture that supports information security is critical. Ensuring that all members of an organization understand their responsibilities in protecting information as well as establishing a culture that supports compliance with security practices can improve the overall effectiveness of information security systems. (Grant Solomon, 2020)

By implementing these suggestions, organizations can develop a stronger and more effective information security culture, as well as improve their overall understanding and application of technology in support of their goals and operations.

4. CONCLUSION

The results of this study indicate that there are significant differences in the level of awareness, knowledge, compliance and behavior related to information security between various types of organizations. Organization A, which operates entirely in IT, demonstrated the best results in all categories, reflecting excellent understanding and application of technology as well as a strong commitment to information security standards. In contrast, Organization B, as a non-IT organization that uses IT in its operations, and Organization C, which is also non-IT but uses IT to a limited extent, showed lower scores, with Organization B having the lowest results in all categories and Organization C showing better results but still less than optimal.

These findings confirm that the level of understanding and application of IT is closely related to the focus and commitment to technology owned by the organization. IT-focused organizations have an advantage when it comes to integrating and implementing technologies that support information security. On the other hand, non-IT organizations, especially those using technology in a limited or secondary capacity, often face challenges in increasing awareness, knowledge, and compliance with information security practices.

To improve an information security culture, organizations need to focus on several key areas: increasing IT-related training and education, strengthening security policies and procedures, investing in IT resources, increasing technology integration in operations, and building an organizational culture that supports information security. By implementing these steps, organizations can address existing deficiencies, increase the effectiveness of information security, and support better data and information protection.

REFERENCES

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

Akhyari Nasir, RA (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, SM (2021). An Empirical Analysis of the Information Security Culture Key Factors Framework. Computers & Security.

Alan Dennis, B. H. (2019). Systems Analysis and Design with UML. John Wiley & Sons.

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

Alifiani Kurniati, LE (2020). Information Technology Risk Management on e-Government: Systematic Literature Review (Information Technology Risk Management on e-Government: Systematic Literature Review). JURNAL IPTEKKOM (Journal of Information Science & Technology), 207-222.

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

Choe, AI-D. (2019). A Framework of Information Security Integrated with Human Factors. International Conference on Human-Computer Interaction, 217–229.

Ehab Al-Shaer, R.B. (2019). Network Security: A Practical Approach. Morgan Kaufmann.

Gallaugher, J. (2020). Information Systems: A Manager's Guide to Harnessing Technology. FlatWorld.

Grant Solomon, IB (2020). The influence of organizational culture and information security culture on employee compliance behavior. Journal of Enterprise Information Management.

Harkins, M. (2019). Managing Risk and Information Security: Protect to Enable. Apress.

Hyungjin Lukas Kim, AH (2019). Protecting intellectual property from insider threats. Journal of Intellectual Capital, 181-202.

J Zaburko, JS-C. (2019). Information Security Risk Assessment Using The AHP Method. Materials Science and Engineering, 1-11.

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*.

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.