International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||12||Pages||8141-8149||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i12.em12

Factors Influencing Information Security Culture in Organizations Dealing With Economic Crime in Kenya

John Onyango Abingo[1], Dr.George Musumba[2], Dr.Anthony Maina Mbuki[3]

[1]Student Master of Science in Forensic and Security Management, Cyber Crime Forensics Option, Institute of Criminology, Forensic and Security Studies, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

[2] Lecturer Institute of Computer Studies and Information Technology, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

[3] Lecturer Institute of Computer Studies and Information Technology, Dedan Kimathi University of Technology, Nairobi Campus, Loita Street, Pension Towers, 2nd Floor, Kenya

Abstract:
Information security culture is very important for any organization, especially in the public sector, where sensitive information is regularly processed and stored. This importance has become more pronounced in recent years because the frequency and sophistication of cyber-attacks have increased, highlighting the need for effective information security measures such as control policies including access controls, password regulations. However, the success of these measures depends on the development of a strong information security culture within the organization. This study thus aimed to establish the organizational factors influencing information security culture in the organization dealing with economic crime in Kenya. The study focused on information security control, organization structure and organizational culture and how they influence information security culture. The study was underpinned on Security Culture Framework, CIA triad model, structural contingency theory and organizational culture theory. Descriptive research design was adopted. The study targeted 5729 employees in the Economic crimes investigative organizations in Kenya. Stratified random sampling approach was used to classify the sample frame. Simple random sampling technique was utilized to select respondents from each stratum to come up with a sample size of 361 respondents. Data was gathered from the five organizations located in Nairobi County, using self-administered questionnaires. The questionnaires were distributed through a drop and pick-up method, wherein the researcher personally delivered them to the respondents at their workplace. The study produced quantitative data that was coded and entered into Statistical Packages for Social Scientists (SPSS Version 26) for analysis, using both descriptive and inferential statistics. The quantitative data was presented using tables and graphs, with accompanying explanations in prose. The study concludes that information security control has a positive and significant effect on information security culture in five selected state-owned organizations dealing with economic crime in Kenya. In addition, the study concludes that organization structure has a positive and significant effect on information security culture in five-selected state-owned organization dealing with economic crime in Kenya. Further, the study concludes that organizational culture has a positive and significant effect on information security culture in five-selected state-owned organization dealing with economic crime in Kenya. Based on the study findings, the study recommends that the management of state-owned organization dealing with economic crime in Kenya should establish a dedicated and well-defined information security governance structure. This involves creating a specialized information security department or team that reports directly to top management, ensuring that information security is prioritized at the highest organizational level.

Keywords: Information security culture, information security control, organization structure and organizational culture**.**

1. Introduction

1.1. Background of the Study

Information technology has brought about massive opportunities for organizations across the world. Information assets for instance can now be shared across boundaries in a faster and more efficient manner using information technology (Alzahrani & Kavita, 2021). However, the use of information technology systems has also made information security breaches easier. An occurrence of information security breaches arises when there is inadequate protection of information, enabling unauthorized individuals to gain access to it. Such breaches can have significant ramifications. In the context of organizations, a breach typically results in substantial financial setbacks, expensive legal battles, harm to reputation, and in severe instances, loss of business opportunities (Astakhova, 2020). The primary objective of information security is to safeguard the confidentiality, integrity, and availability of the information infrastructure. It involves ensuring that information is protected from both unintentional and intentional misuse. Thus to ensure that organisations survive, it is important that they safeguard their information assets from these information security threats by creating a protective information security culture (Gyllensten & Torner, 2021).

Information security culture refers to a system of security-focused norms, values, attitudes, and assumptions that are embedded in the regular functioning of an organization and are manifested through the conduct and actions of all individuals and entities associated with the organization (da Veiga, Astakhova, Botha, & Herselman, 2020), (Chopra & Chaudhary, 2020). According to da Veiga et al., (2020), information security culture is a combination of perceptions, attitudes, values, assumptions, and knowledge that guide employees in exhibiting appropriate information security behaviour. The ultimate objective of developing a strong information security culture is to manage and minimize information security risks to safeguard the organization's information assets and accomplish its overall objectives (Bednar & Welch, 2020).

A strong information security culture is essential for effectively implementing and maintaining the principles of the Information Security Triangle, confidentiality, integrity, and availability (CIA) (Tenzin, 2021). Confidentiality refers to the protection of sensitive information from unauthorized disclosure. A strong security culture emphasizes the importance of confidentiality by establishing policies and procedures to control access to sensitive information, such as passwords, personal information, and trade secrets. Employees should be trained on the importance of keeping confidential information confidential and be held accountable for any breaches of confidentiality.

Integrity on the other hand refers to the protection of information from unauthorized modification or deletion (Assefa & Tensaye, 2021). A strong security culture emphasizes the importance of data integrity by ensuring that data is accurate and reliable, and that it has not been tampered with or altered in any way. This can be achieved through the implementation of access controls, data backup and recovery procedures, and data validation processes. da Veiga, Astakhova, Botha, and Herselman (2020) averred that employees should be trained on the importance of maintaining data integrity and be held accountable for any breaches of integrity. Availability refers to the ability to access information when it is needed. A strong security culture emphasizes the importance of availability by ensuring that critical systems and data are available when they are needed (Chopra & Chaudhary, 2020). This can be achieved through the implementation of redundancy, backup and recovery procedures, and disaster recovery plans. Employees should be trained on the importance of maintaining system availability and be held accountable for any breaches of availability. Organizations can thus build a culture that prioritizes information security and minimizes the risk of security breaches by emphasizing the importance of each of these domains and implementing appropriate policies, procedures, and training (Chopra & Chaudhary, 2020).

To enhance information security culture, it is crucial to identify the factors that influence it. Several authors have explored these factors with varying findings. In in Saudi Arabia, AlGhamdi, Win and Vlahu-Gjorgievska (2021) explored employees' intentions toward complying with information security controls in public organisations. They identified the severity of punishment and certainty of detection as some of the factors that influence employees' intentions toward complying with information security controls. In USA, Carver (2020) proposed a framework for how organisations may attend to key factors influencing organisational culture to facilitate and nurture a well-prepared information security culture. He opined that by defining the meaning of organisational culture and understanding what a desirable culture should include, businesses can enhance their ability to identify issues, create remedies, and foster more positive environments. According to Carver (2020) the cultural alignment of the organization sets the standards for appropriate system and leadership behaviors that are necessary to successfully execute the enterprise's strategy. As a result, employee behavior and interactions are shaped by this cultural alignment. The study however, did not clearly establish the influence of organizational culture on information security culture, which the current study seeks to do.

In the UK, Tolah (2021) developed a framework for understanding and establishing an effective information security culture. In the framework, a security culture is made up of different elements that fall into three groups: influential factors, organizational behavior factors that shape a security culture and reflection factors that make up a security culture (Tolah, 2021). The first group includes top management, security policy, security education and training, security risk analysis and assessment, and ethical behavior. The second group includes personality traits and job satisfaction, while the third group includes security awareness, security ownership, and security compliance. This framework however only identified and categorised the factors but did not clearly show their influence on the organizational information security culture.

In Ethiopia, Abebe and Lessa (2020) explored the human factors influence on information security culture at commercial banks. Their study demonstrated that employees' conduct regarding technology usage, perception, and information system security can be positively influenced through information security training. They opined that providing information security training can enhance employees' behavior regarding the information systems security. This type of training can specifically address human factor issues within banks by enhancing users' theoretical and practical knowledge (Abebe & Lessa, 2020). Because information systems rely on human interaction, it is crucial to involve users in the information systems security process.

Locally, Njoroge (2020) also studied the human factors affecting favourable information security culture in small and medium-sized enterprises in Kenya. The study established that top management support and involvement together with reward and deterrence measures are positive and significant predictors of favorable information security culture. The study also found that information security policy, information security change management, information security training and awareness programs, security monitoring and audit also have positive effect on favorable information security culture.

1.2. Statement of the Problem

It is important for one to note that the importance of information security and information security culture is clear from the word go. This is especially so for public organizations, which hold a vast amount of sensitive information that, must be protected from unauthorized access, use, disclosure, and destruction. However, despite the implementation of various information security controls, public organizations continue to face significant information security threats (Nasir et al., 2019). Despite the increasing recognition of the importance of information security culture, there has been a lack of adequate research in this area in Kenya. Studies by Carver (2020) which is limited to organizational culture, Tolah (2021) which only identified and categorized the factors but did not clearly show their influence on the organizational information security culture and Abebe and Lessa (2020) which focused on commercial banks; are limited in scope and provided fragmented findings on the different factors influencing information security culture. This study aims to focus on information security control, organization structure and organizational culture and how they influence information security culture specifically in five selected state-owned organizations dealing with economic crime in Kenya. Riebe, Kaufhold, and Reuter (2022) and Solomon and Brown (2021) looked at these factors and established that effective information security controls are essential to minimize the risk of information security incidents, and that a clear and well-defined organizational structure that delineates the roles and responsibilities of individuals and departments responsible for implementing and maintaining information security controls. However, these factors were studied individually and the studies were located in developed jurisdictions with different contextual characteristics from Kenya.

While studies such as Mahfuth, et al., (2017) exploration of the factors affecting information security culture, Mohd, et al., (2012) examination of factors influencing information security culture among ICT librarians, and Bojmaeh (2015) investigation into the main factors impacting information security in developed countries have been conducted, they have primarily focused on general factors affecting information security culture. Additionally, these studies were conducted outside of Kenya and may not reflect the local context. Therefore, the present study aimed to determine the factors influencing information security culture in five selected state-owned organization dealing with economic crime in Kenya.

1.3 . Purpose of the Study

To assess the influence of information security control on information security culture in five selected state-owned organizations dealing with economic crime in Kenya

2. Literature Review

2.1. Theoretical literature Review

The study exploring the information security control variable and its influence on information security culture in organizations dealing with economic crime in Kenya utilized the CIA Triad model. The CIA Triad is a foundational model in information security, revolving around the principles of confidentiality, integrity, and availability (CIA) (Jan Eloff, 2020). Confidentiality focuses on protecting data from unauthorized access, employing mechanisms such as authentication, encryption, and user authentication methods like two-factor authentication (2FA) (Hanifah & Nuradli, 2020).

Integrity ensures the consistency, accuracy, and trustworthiness of data throughout its lifecycle. Techniques such as file permissions, version control, checksums, and digital signatures are utilized to prevent unauthorized changes to data (Da Veiga & Eloff, 2019). Availability ensures that information is consistently accessible to authorized parties, addressing issues like power outages, system failures, and denial of service attacks (DoS). Measures for ensuring availability include maintaining hardware and technical infrastructure, monitoring bandwidth usage, regular software patching, and implementing disaster recovery plans (Njoroge, 2020).

The CIA Triad serves as a foundational framework for developing security policies, guiding security strategies, and implementing controls in organizations. It helps identify problem areas and solutions in information security, providing a comprehensive approach to managing security risks effectively (D'Arcy & Greene, 2019).

2.2. Conceptual Framework

A conceptual framework is a theoretical structure that outlines the key concepts, ideas, and assumptions that underlie a particular research study. It serves as a roadmap for researchers, helping them to identify the key variables, concepts, and relationships that need to be explored in order to answer their research questions. This study's conceptual framework identifies the key variables as illustrated in figure 2.1

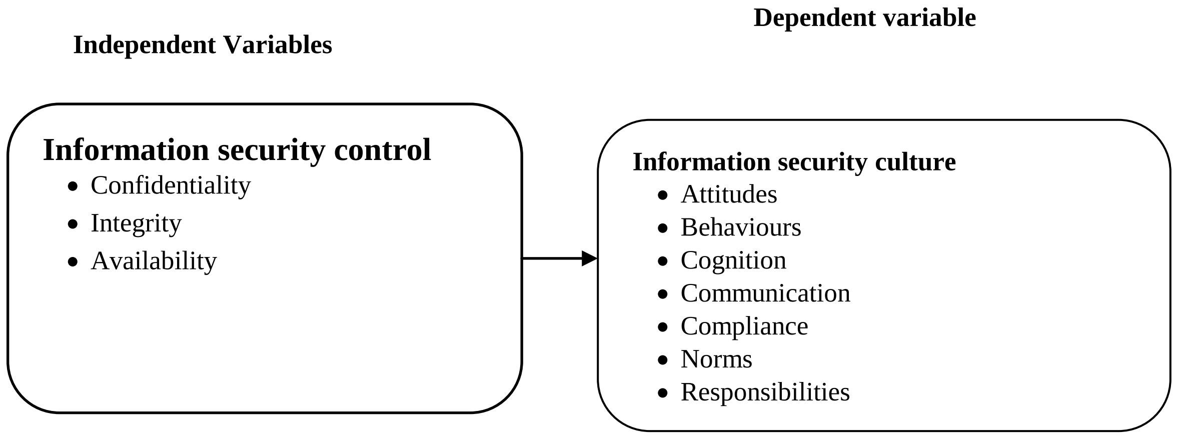

Figure 2. 1: Conceptual Framework

3. Methodology

The study adopted a quantitative approach with a survey containing closed-ended questions.

The target population was 5,729 comprising of organization dealing with Economic crime in Kenya. A sample was selected from a population of 5,729 using stratified random sampling to ensure adequate representation of each stratum within the population.

3.1 Table 1

Institution	Target Population	Sample size
Ethics & Anti-Corruption Commission	750	47
DCI	280	18
Asset Recovery Agency	120	8
Kenya Revenue Authority	4,461	281
Financial Reporting Centre	118	7
Total	**5729**	**361**

The primary method of data collection in this study involved using a structured questionnaire. The questionnaires were distributed through a drop and pick-up method, wherein the researcher personally delivered them to the respondents at their workplace. If respondents were unable to complete the questionnaire immediately, the researcher leaved the questionnaires with them and returned later to collect them. The study produced quantitative data that was coded and entered into Statistical Packages for Social Scientists (SPSS Version 26) for analysis, using both descriptive and inferential statistics. The descriptive statistics involved calculating absolute and relative frequencies (percentages), measures of central tendency, and dispersion (mean and standard deviation, respectively). The quantitative data was presented using tables and graphs, with accompanying explanations in prose. Qualitative data analysis focused on the content of the responses, identifying recurring themes or patterns and organizing them into meaningful categories and presentation done in prose.

The study utilized Karl Pearson's correlation coefficient and multiple regressions to establish the connection between the independent and dependent variables. A correlation analysis was conducted to determine the degree of interdependence between the variables. A positive coefficient indicated that as the value of the independent variable increases, the mean of the dependent variable also increased. A negative coefficient suggested that as the independent variable increases, the dependent variable decreases. Furthermore, a multiple regression analysis was performed using the regression equation which will be as follows:

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \varepsilon}$$

The variables for the study are defined as follows:

The dependent variable, Y, is the information security culture.

X1 represents the independent variable, information security controls.

For normality test in this research, Shapiro Wilk test was utilized by the researcher. The data was considered normally distributed if the significant value (p-value) > 0.05, on the contrary the null hypothesis was rejected if the value is < 0.05, which implied that there is normal distribution of data.

Analysis of variance (ANOVA) was utilized in testing for Linearity in the determination of the correlation between dependent and independent variables. A deviation form linearity > 0.05 was a depiction that the relationship between the dependent and independent variables are linearly interrelated whereas if it was < 0.05 it indicated that the relationship is not linear.

4. Study Findings and Discussion

The study sought to assess the influence of information security control on information security culture in five selected state-owned organizations dealing with economic crime in Kenya,

4.1 Descriptive Statistics

The study found that information security control has a positive and significant effect on information security culture in five-selected state-owned organization dealing with economic crime in Kenya. From the results, the respondents agreed that confidentiality is ingrained in the organizational culture as a fundamental aspect of information security. In addition, the respondents agreed that the organization emphasizes data accuracy and reliability as critical elements of its information security policies. Further, the respondents agreed that the organization implements measures to protect against denial-of-service (DoS) attacks or other threats that compromise availability. From the results, the respondents agreed that employees consistently verify and validate data to ensure its accuracy and integrity. In addition, the respondents agreed that the organization proactively monitor systems and resources to prevent potential availability issues. Further, the respondents agreed that there are robust encryption and security measures in place to protect confidential data

4.2 Correlation Analysis

This research adopted Pearson correlation analysis to determine how the dependent variable (information security culture) relates with the independent variables (information security control).

Table 4. 1: Correlation Coefficients

		Information Security Culture	**Information Security Control**
Information Security Culture	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	280	
Information Security Control	Pearson Correlation	.843	1
	Sig. (2-tailed)	.000	
	N	280	280

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

From the results, there was a very strong relationship between information security control and information security culture in five selected state-owned organization dealing with economic crime in Kenya (r = 0. 843, p value =0.000). The relationship was significant since the p value 0.00 was less than 0.05 (significant level). The findings are in line with the findings of Hanifah and Nuradli (2020) who indicated that there is a very strong relationship between information security control and information security culture.

4.3 Regression Analysis.

Multivariate regression analysis was used to assess the relationship between independent variables (information security control) and the dependent variable (information security culture).

Table 4. 3: Model Summary

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.877[a]	.769	.767	.10412

The model summary was used to explain the variation in the dependent variable that could be explained by the independent variables. The r-squared for the relationship between the independent variables and the dependent variable was 0.769. This implied that 76.9% of the variation in the dependent variable (information security culture in five-selected state-owned organization dealing with economic crime in Kenya) could be explained by independent variables (information security control, organization structure and organizational culture).

4.4 Analysis of Variance

Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	102.028	3	34.3	700	.002[b]

	Residual	13.653	276	.049		
	Total	115.681	279			
a. Dependent Variable: information security culture in five selected state-owned organization dealing with economic crime in Kenya						
b. Predictors: (Constant), information security control.						

The ANOVA was used to determine whether the model was a good fit for the data. F calculated was 700 while the F critical was 2.637. The p value was 0.002. Since the F-calculated was greater than the F-critical and the p value 0.002 was less than 0.05, the model was considered as a good fit for the data. Therefore, the model can be used to predict the influence of information security control on information security culture in five-selected state-owned organization dealing with economic crime in Kenya.

Table 4. 5: Regression Coefficients

	Unstandardized Coefficients		**Standardized Coefficients**	**t**	**Sig.**
	B	Std. Error	Beta		
(Constant)	0.202	0.051		3.960	0.002
information security control	0.364	0.092	0.365	3.957	0.003

a. Dependent Variable: information security culture in five-selected state-owned organization dealing with economic crime in Kenya

According to the results, information security control has a significant effect on information security culture in five selected state-owned organization dealing with economic crime in Kenya β_1=0.364, p value= 0.003). The relationship was considered significant since the p value 0.003 was less than the significant level of 0.05. The findings are in line with the findings of Hanifah and Nuradli (2020) who indicated that there is a very strong relationship between information security control and information security culture.

5. Conclusions and Recommendations

5.1 Conclusion

The study found that information security control has a positive and significant effect on information security culture in five-selected state-owned organization dealing with economic crime in Kenya. From the results, the respondents agreed that confidentiality is ingrained in the organizational culture as a fundamental aspect of information security. In addition, the respondents agreed that the organization emphasizes data accuracy and reliability as critical elements of its information security policies. Further, the respondents agreed that the organization implements measures to protect against denial-of-service (DoS) attacks or other threats that compromise availability. From the results, the respondents agreed that employees consistently verify and validate data to ensure its accuracy and integrity. In addition, the respondents agreed that the organization proactively monitor systems and resources to prevent potential availability issues. Further, the respondents agreed that there are robust encryption and security measures in place to protect confidential data.

The study concludes that information security control has a positive and significant effect on information security culture in five-selected state-owned organization dealing with economic crime in Kenya. Findings revealed that confidentiality, integrity and availability influence information security culture in five selected state-owned organization dealing with economic crime in Kenya.

5.2 Recommendations

The study recommends that the management of state-owned organization dealing with economic crime in Kenya should implement a comprehensive and continuous information security awareness and training program. This program should be tailored to educate all employees, from top management to operational staff, on the importance of information security practices, the risks associated with data breaches, and the specific security protocols relevant to their roles

References

1. Abebe, G., & Lessa, L. (2020). *Human Factors Influence On Information Systems Security At Commercial Banks In Ethiopia.* Addis Ababa : Masters thesis, Addis Ababa University.
2. AlGhamdi, S., Win, K., & Vlahu-Gjorgievska, E. (2021). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Government Information Quarterly*, 39(4), 1-14.
3. Alzahrani, L., & Kavita, P. S. (2021). The Impact of Organizational Practices on the Information Security Management Performance. *Information*, 12(10), 398.
4. Apolinário, S., Yoshikuni, A. C., & Larieira, C. (2023). Resistance to information security due to users' information safety behaviors: Empirical research on the emerging markets. *Computers in Human Behavior*, 145, 107772.
5. Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: an institutional perspective. *Ethiop. J. Sci*, 44(1):108–118.
6. Bednar, P. M., & Welch, C. (2020). Socio-Technical Perspectives on Smart Working: Creating Meaningful and Sustainable Systems. *Information Systems Frontiers*, 22, pages281–298.
7. Bell, E., Bryman, A., & Harley, B. (2018). *Business research methods.* Oxford university press.
8. Carver, R. (2020). A framework for fostering a dynamic information security culture. *Cyber Security: A Peer-Reviewed Journal, Henry Stewart Publications*, 4(2), 145-159.
9. Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System Management System. *Implementing an Information Security*, https://doi.org/10.1007/978-1-4842-5413-4.
10. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design (international student edition): Choosing among five approaches. *Language*, *25*(1), 459
11. Crossler, R., Andoh-Baidoo, F., & Menard, P. (2019). Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: study of US and Ghana. *Inf. Manag.*, 56 (5), 754-766.
12. da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining Organizational Information Security Culture-Perspectives from Academia and Industry . *Computers and Security* , https://doi.org/10.1016/j.cose.2020.101713.
13. Dasgupta, S., & Gupta, B. (2019). Espoused organizational culture values as antecedents of internet technology adoption in an emerging economy. *Inf. Manag.*, 56 (6), 103142.
14. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Comput. Secur.*, 92, 101747. .
15. Geffner, R., Shaw, M., & Crowell, B. (2018). Ethical considerations in forensic evaluations in family court. In M. M. Leach, & E. R. Welfel, *Cambridge handbooks in psychology. The Cambridge handbook of applied psychological ethics* (pp. 452–473). London: Cambridge University Press.
16. Gyllensten, K., & Torner, M. (2021). The role of organizational and social factors for information security in a nuclear power industry. *Organizational Cybersecurity Journal: Practice, Process and People*, 2(1), 3-20.
17. Hair, J. F., Celsi, M. W., Money, A. H., Samouel, P., & Page, M. J. (2015). *Essentials of Business Research Methods.* Oxfordshire, England: Routledge.
18. Kamariza, Y. (2017). *Implementation of information security policies in public organizations : success factor.* Jonkoping University.
19. Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security.* (3rd ed.). Jones & Bartlett Learning, LLC, an Ascend Learning Company.
20. Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. H. (2020). Information security policy compliance : Leadership, trust, role values, and awareness. *Journal of Computer Information Systems*, 60(1), 1-8.

21. Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information management*, 54, 1-12.
22. Mehrad, A., & Tahriri, M. (2019). Comparison between qualitative and quantitative research approaches: Social sciences. *International Journal For Research In Educational Studies*, 5(7), 1-7.
23. Meyers, L. S., Gamst, G., & Guarino, A. J. (2016). *Applied Multivariate Research: Design and Interpretation.* Washington, DC: Sage Publishing.
24. Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2020). Information security culture for guiding employee's security behaviour: A pilot study. *Sixth International Conference on Information Management* (pp. 205-209). London: United Kingdom.
25. Nasir, A., Arshah, R., Ab Hamid, M., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review . *Journal of information security and applications*, 44, 12-22.
26. Njoroge, G. M. (2020). *Human Factors Affecting Favourable Cybersecurity Culture- a Case of Small and Medium-sized Enterprises Smes Providing Enterprise Wide Information Systems Solutions in Nairobi City County in Kenya.* Nairobi: Faculty of Science & Technology (FST), University of Nairobi.
27. Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, 59(3), 211-217.
28. Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students.* London, United Kingdom: Pearson Education Limited.
29. Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, 120, 102774.
30. Suharyanto, A., & Lestari, R. (2020). The Fall and Rise of The Contingency Theory of Leadership. *Iapa Proceedings Conference*, 423, DOI:10.30589/proceedings.
31. Suriani, M. (2017). *A model of factors influencing information security culture in oil and gas company.* Universiti Teknologi Malaysia: Masters thesis, Razak Faculty of Technology and Informatics.
32. Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management*, 18-27.
33. Tenzin, S. (2021). *An Investigation of the Factors that Influence Information Security Culture in Government Organisations in Bhutan.* Perth, Western Australia: Doctor of Information Technology thesis, Murdoch University.
34. Tolah, A. (2021). *A Framework for Understanding and Establishing an Effective Information Security Culture.* Plymouth, England: Doctor Of Philosophy thesis, University of Plymouth.
35. Zaini, M., Harun, Q., & Masrek, M. (2018). The Development Of An Information Security Culture Scale For The Malaysian Public Organization. *International Journal of Mechanical Engineering and Technology (IJMET),* 9(7), 1255–1267.