ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 4, pp: (68-72), Month: October 2022 - December 2022, Available at: www.researchpublish.com

THE IMPACT OF CYBERSECURITY STANDARD GUIDELINES ON THE CULTURE OF CYBERSECURITY

[1]Jamilu Garba, [2]Jasber Kaur

[1,2] Universiti Teknologi Mara

DOI: https://doi.org/10.5281/zenodo.7484002

Published Date: 26-December-2022

Abstract: **This paper examines factors that significantly affect the use of cybersecurity culture by banks in Nigeria. One of these factors was the cybersecurity standard guidelines. This study adopted a quantitative approach to reaching its objectives by using questioner that provides a framework for building hypotheses. Fifty participants from different banks in Nigeria participated in the study. After reviewing several relevant studies, a five-point Likert scale questionnaire was designed to collect the required data, which was analyzed using SPSS. Hypotheses were tested to see which results could then be generalized. The result showed the regression coefficients of the variable cybersecurity standard guidelines explain (79.2%) of the variance in the culture of cybersecurity this interpretation is statistically significant at the level (0.05), and the table shows that the values of the regression coefficients were positive and statistically significant between the cybersecurity standard guidelines and culture of cybersecurity (β = 0.813; t = 26.356; p = 0.000); The square of the overall correlation coefficient R2 between cybersecurity standard guidelines and culture of cybersecurity was (0.792), which means that the independent variable affects 79.2% of the variance in the culture of cybersecurity as the dependent variable. Thus, we accept the H1 hypothesis. The researchers recommend the use of new variables and factors in studying the relationships that affect cybersecurity and studying the extent of culture that people have about this concept in different environments and countries, in addition to different sectors.**

Keywords: **Cybersecurity Culture, Cybersecurity standard guidelines.**

1. BACKGROUND

Cybersecurity guidelines is the organization document usually drafted by chief cybersecurity officer of the organization to prevent or mitigate cybersecurity vulnerability (Yani, 2016; Lubua & Pretorius, 2019). The creation of cybersecurity culture will begin with the creation of the organization's cybersecurity guidelines, followed by the creation of cybersecurity architecture and detailed cybersecurity blueprint (Liu et al., 2020). The organization cybersecurity effort can be succeeded only if it operate in conjunction with the organizational cybersecurity standard guidelines (Papazoglou 2019). Without cybersecurity standard guidelines, the organization will be unable to meet the cybersecurity needs of the various communities of interest including management from all communities, general staff and public users (Masrek et al., 2017). According to Nasir et al., (2020) organization with lack cybersecurity standard guidelines clearly shows that it lacking proper cybersecurity guidance, and showing a low level of senior management commitment to cybersecurity. Cybersecurity standard guidelines should be regularly reviewed at the organizational level to determine whether it satisfied cybersecurity needs and incorporated into the working environment so that it becomes a part of the individual's daily activities (Alshaikh, 2020 & Uchendu et al., 2021). The Individuals can use cybersecurity standard guidelines to learn about the acceptable level of cybersecurity behaviour required to keep personal data secure (Tolah et al., 2017) .

However, the guidelines were examined in terms of how it should be written, how to encourage the users to follow the guidelines, and how the guidelines influence an organization's cybersecurity culture. The cybersecurity guidelines is considered as a significant strategy for monitoring cybersecurity in organizations and businesses. Veiga et al (2021) carried out a survey to determine the impact of cybersecurity standard guidelines on cybersecurity culture by relating organizations with security standard guidelines and those without security standard guidelines. The finding shows that cybersecurity has been increased in organizations where cybersecurity standard guidelines implemented.

The foundation for shared cybersecurity values and beliefs among users is provided by cybersecurity standard guidelines (Yıldırım and Mackie 2019). Users are expected to follow cybersecurity standard guidelines that communicate desired cybersecurity behaviour (Mannan and Van Oorschot 2018). Users are often under the impression that implementing or adhering to cybersecurity standard guidelines will reduce cyberthreats (Gcaza and von Solms 2017). Users who follow cybersecurity standard guidelines may be able to protect their data from cyberthreats and risks. Virus attacks occurred in 80% of the organizations surveyed because users were unaware of or failed to follow cybersecurity standard guidelines.

Cybersecurity standard guidelines have been identified as one of the factors influencing the development of an effective cybersecurity culture by researchers. Hengstler and Pryazhnykova (2021) used the Theory of Planned Behaviour to develop a research model to identify the factors that influence the intention to follow standard computer security policy. The researcher discovered a connection between having standard computer security guidelines and the intention to follow them, which is mediated by attitude and belief. This model was later tested by Acuna (2018), who discovered that computer security guidelines influenced users' intention to follow computer security regulations, and this relationship was mediated by cybersecurity culture's attitude and belief. Furthermore, Veiga (2017) conducted an empirical study over an eight-year period to assess cybersecurity culture in twelve countries. As a result, the current paper will decide to use a mixed method approach and focuses on developing a reliable and valid cybersecurity culture measurement model by identifying the human factors that influencing cybersecurity culture.

2. THE RESEARCH QUESTION, AIM, AND HYPOTHESIS

Based on the background of the study and a review of the previous literature, the following question was formulated:

- Is there an impact of cybersecurity standard guidelines on the culture of cybersecurity?

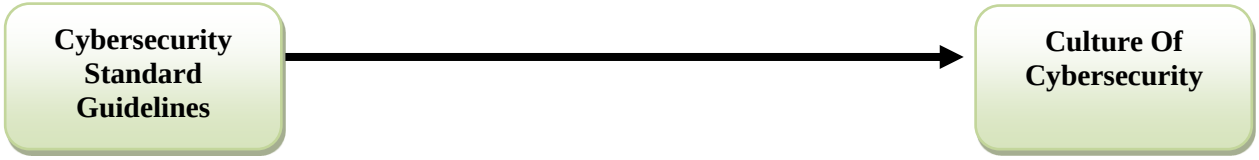
The aim of this question is:

- Studying the relationship and influence between cybersecurity standard guidelines and cybersecurity culture.

Through the background of the study, the study question, and the aim of the study, the following hypothesis was formulated

- H1: There is a statistically significant effect of the influence of cybersecurity standard guidelines on the culture of cybersecurity.

3. CONCEPTUAL FRAMEWORK



4. THEORETICAL FRAMEWORK

A theoretical framework refers to the structure that can hold or support research works (Uchendu et al., 2021). It will help to explain why the problem in the research exists. And the theoretical framework that will guides the researcher to determine what things will be measure, and what statistical relationships will be looking for. The theory of reasoned action (TRA) developed by Fishbein & Ajzen, (1975), and Later, Ajzen (1991) extended the theory to theory to planned behavior by adding perceived behavioral control. The primary goal of the theory of reasoned action and theory of planned behaviour is to explain the relationship between attitudes and behaviors and has shown significant results in predicting behavioral intentions and some committed behaviors (Fishbein and Ajzen 1975).

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 4, pp: (68-72), Month: October 2022 - December 2022, Available at: www.researchpublish.com

5. METHODOLOGY

This study selected fifty participants from banks in nigeria to be participants. The data was obtained online (online questionnaires on the www.surveyshare.com site), and the questionnaire includes one part this section contains twenty basic designs that are linked to cybersecurity standard guidelines and the culture of cybersecurity

6. INSTRUMENT'S RELIABILITY

the test determines the reliability. Gay and Airasian (2005) mentioned reliability determine the level at which the test measures what is constant. Furthermore, the basic consistent quality of the internal consistency of the information contained in the study is estimated using Alpha Cronbach's (Cronbach, 1984). Alpha Cronbach's value can be expanded in a number of things or a natural relationship.

Table 1: Scale Reliability Questionnaire

Variable	N. of Items	Alpha (a)
Cybersecurity Standard Guidelines	10	0.892
Culture Of Cybersecurity	10	0.914

7. HYPOTHESES TESTING

This research proposed hypothesis in an attempt to examine the relationships among the factors of the proposed model. Here, the mean values of the variables are determined within the factors or constructs. The values obtained were then evaluated for correlation. All hypothesis tests show that there is a positive relationship between structures. A positive correlation ranging from zero and satisfying the above minimum criteria thus supports both the hypothesis and the relationship.

We seek to test a hypothesis (H1: There is a statistically significant effect of the influence of cybersecurity standard guidelines on the culture of cybersecurity). To check this hypothesis, linear regression coefficients were extracted and the following table shows these results:

Table 2: Hypotheses Testing

Sample	Non-standard		β	T value	Statistical significance	R	R2	F value	significance
	Reg.	S. E							
Fixed	1.284	.124		19.102	.000	.847	.792	753.222	.000*
	.802	.031	.813	26.356	.000*				

Table 2 shows the regression coefficients of the variable cybersecurity standard guidelines explain (79.2%) of the variance in the culture of cybersecurity this interpretation is statistically significant at the level (0.05), and the table shows that the values of the regression coefficients were positive and statistically significant between the cybersecurity standard guidelines and culture of cybersecurity ($\beta = 0.813$; $t = 26.356$; $p = 0.000$); The square of the overall correlation coefficient R2 between cybersecurity standard guidelines and culture of cybersecurity was (0.792), which means that the independent variable affects 79.2% of the variance in the culture of cybersecurity as the dependent variable. Thus, we accept the H1 hypothesis.

8. CONCLUSION

The main objective of cybersecurity standard guidelines research in the context of cybersecurity is to approach, identify, and finally analyze how an individual's cybersecurity standard guidelines , beliefs, and attitudes can affect cybersecurity, either directly or indirectly, intentionally, or unintentionally. Understanding the root of the problem may lead to effective solutions, such as implementing policies and guidelines, along with training programs that can help in mitigating cybersecurity vulnerabilities. However, people of different cybersecurity standard guidelines in the modern world needs to have private information such as password and private information developed to be essentially private and undisclosed, but the sharing of private information is a common practice in some groups or family. This is because of social attitude and trust with whom to share private information with. Cybersecurity standard guidelines played an important role in whether private information would be shared or not. The researcher suggests and recommends the use of new variables and factors in studying the relationships that affect cybersecurity, and studying the extent of culture that people have about this concept

in different environments and countries, in addition to different sectors. However, the guidelines were examined in terms of how it should be written, how to encourage the users to follow the guidelines, and how the guidelines influence an organization's cybersecurity culture. The cybersecurity guidelines are considered as a significant strategy for monitoring cybersecurity in organizations and businesses. The researchers recommend the use of new variables and factors in studying the relationships that affect cybersecurity and studying the extent of culture that people have about this concept in different environments and countries, in addition to different sectors.

REFERENCES

[1] Adele, Veiga. 2017. "Employees Who Had Read the Information Security Policy Accepted Manuscript (Unedited)." Information & Computer Security (June 2016).

[2] Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

[3] Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. Psychological bulletin, 82(2), 261.

[4] Alshaikh, Moneer. 2020. "Computers & Security Developing Cybersecurity Culture to Influence Employee Behavior : A Practice Perspective." computer & security 98.

[5] Chowdhury, Noman H., Marc T.P. Adam, and Timm Teubner. 2020. "Time Pressure in Human Cybersecurity Behavior: Theoretical Framework and Countermeasures." Computers & Security 97: 101963.

[6] Cronbach, L. J. (1984). A research worker's treasure chest. Multivariate behavioral research, 19(2-3), 223-240.

[7] Gcaza, Noluxolo, and Rossouw von Solms. 2017. "A Strategy for a Cybersecurity Culture: A South African Perspective." Electronic Journal of Information Systems in Developing Countries 80(1): 1–17.

[8] Hengstler, Sebastian, and Natalya Pryazhnykova. 2021. "Reviewing the Interrelation Between Information Security and Culture : Toward an Agenda for Future Research." 16th International Conference on Wirtschaftsinformatik, March 2021, Essen, Germany (March): 1–26.

[9] Liu, Cai, Stephen Nicholas, and Jian Wang. 2020. "The Association between Protection Motivation and Hepatitis b Vaccination Intention among Migrant Workers in Tianjin, China: A Cross-Sectional Study." BMC Public Health 20(1): 1–10.

[10] Lubua, Edison Wazoel, and Philip Pretorius. 2019. "Cyber-Security Policy Framework and Procedural Compliance in Public Organisations." Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, Czech Republic, July 23-26, 2019 (August).

[11] Mannan, Mohammad, and P. C. Van Oorschot. 2018. "Security and Usability: The Gap in Real-World Online Banking." Proceedings New Security Paradigms Workshop: 1–14.

[12] Mark, Evans, Yevseyeva Iryna, and Janickle Helge. 2019. "Published Incidents and Their Proportions of Human Error." Information & Computer Security 23(2): 145–60.

[13] Masrek, Mohamad Noorman, Qamarul Nazrin Harun, and Muhammad Khairulnizan Zaini. 2017. "Information Security Culture for Malysian Public Organization: A Conceptual Framework." Proceedings of INTCESS 2017 4th International Conference on Education and Social Sciences (February): 156–66.

[14] Nasir, Akhyari et al. 2020. "Information Security Culture Model for Malaysian Organizations : A Review." International Journal of Advanced Trends in Computer Science and Engineering (1).

[15] Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. Information & Computer Security.

[16] Onwuegbuzie, A. J., & Leech, N. L. (2005). Taking the "Q" out of research: Teaching research methodology courses without the divide between quantitative and qualitative paradigms. Quality and Quantity, 39(3), 267-295.

[17] Papazoglou, Grammatiki Emmy. 2019. "Society and Culture : Cultural Policies Driven by Local Authorities as A Factor in Local Development — The Example of the Municipality of Xanthi-Greece." International Journal of Social Science and Humanity: 2625–39.

[18] Tolah, A, S M Furnell, and M Papadaki. 2017. "A Comprehensive Framework for Cultivating and Assessing Information Security Culture." Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017) (Haisa): 52–64.

[19] Uchendu, Betsy, Jason R.C. Nurse, Maria Bada, and Steven Furnell. 2021. "Developing a Cyber Security Culture: Current Practices and Future Needs." Computers and Security 109.

[20] Veiga, Adéle da, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman. 2020. "Defining Organisational Information Security Culture – Perspectives from Academia and Industry." Computers & Security: 101713. https://doi.org/10.1016/j.cose.2020.101713.

[21] Yani, Yanyan M. 2016. "Cybersecurity Policy and Its Implementation in Indonesia Muhamad Rizal." Journal of ASEAN Studies 4(1): 61–78.

[22] Yıldırım, M., and I. Mackie. 2019. "Encouraging Users to Improve Password Security and Memorability." International Journal of Information Security 18(6): 741–59. https://doi.org/10.1007/s10207-019-00429-y.

[23] Zimmermann, Verena, and Karen Renaud. 2019. "Moving from a 'human-as-Problem" to a 'human-as-Solution" Cybersecurity Mindset." International Journal of Human Computer Studies 131: 169–87. https://doi.org/10.1016/j.ijhcs.2019.05.005.

[24] Zwilling, Moti et al. 2020. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study." Journal of Computer Information Systems 00(00): 1–16. https://doi.org/10.1080/08874417.2020.1712269.