Nigerian Journal of Technology (NIJOTECH)
Vol. 42, No. 3, September, 2023, pp.399 - 405
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v42i3.13

DESIGN OF A CONCEPTUAL FRAMEWORK FOR CYBERSECURITY CULTURE AMONGST ONLINE BANKING USERS IN NIGERIA

AUTHORS:
J. Garba[1,*], J. Kaur[1], and E. Nuraihan Mior Ibrahim[1]

AFFILIATIONS:
[1]College of Computing, Informatics, and Media, Universiti Teknologi Mara Malaysia

***CORRESPONDING AUTHOR:**
Email: jamilugarba2223@gmail.com

ARTICLE HISTORY:
Received: 11 July, 2023.
Revised: 09 October, 2023.
Accepted: 17 October, 2023.
Published: 01 November, 2023.

KEYWORDS:
Conceptual model, Cybersecurity culture, Human factors, Nigeria, Online banking.

ARTICLE INCLUDES:
Peer review

DATA AVAILABILITY:
On request from author(s)

EDITOR:
Ozoemena Anthony Ani

FUNDING:
None

Abstract

This study aims to construct a comprehensive conceptual framework that elucidates the critical human factors influencing cybersecurity culture among online banking users in Nigeria. The research methodology is grounded in a meticulous examination of existing literature in the cybersecurity culture domain, serving as the foundation for this framework. The literature review reveals a conspicuous absence of academic research on cybersecurity culture within Nigeria and underscores the importance of comprehending its unique nuances. Key findings from the literature review highlight the prominence of "cybersecurity awareness," "cybersecurity policy," and "cybersecurity education" as influential factors. "Cybersecurity awareness" emerges as the most pivotal factor due to its recurrent emphasis and recognized centrality. "Cybersecurity policy" and "cybersecurity education" secure the second and third positions, respectively, due to their acknowledged significance in cultivating a security-conscious mindset among online banking users. Furthermore, the literature review exposes a research gap concerning the requisite "cybersecurity knowledge" that should permeate organizations and individuals to augment cybersecurity culture. Additionally, it reveals the underexplored influence of "social norms" and "interpersonal trust" in molding cybersecurity culture. This research accentuates the dearth of cybersecurity culture research within Nigeria and underscores the importance of understanding its unique facets. The proposed conceptual framework provides a valuable resource for designing tailored cybersecurity strategies and programs in Nigeria's online banking sector. It advocates for prioritizing cybersecurity awareness, education, and policy, empowering users with the knowledge and skills needed to safeguard themselves against cyber threats. The model also highlights the relevance of recognizing the role played by social dynamics, interpersonal trust, and social norms in shaping cybersecurity behaviours.

1.0 INTRODUCTION

In recent years, the growth of online banking has been remarkable, transforming the way individuals and businesses conduct financial transactions. Online banking has become a key player in the realm of business activities, offering unparalleled convenience, accessibility, and a wide range of services [1]. The banking industry has embraced this digital shift, adopting uninterruptible banking services to reduce operating costs and enhance customer experience [2]. Online banking in Nigeria has gained significant momentum, fuelled by the dramatic increase in e-commerce applications and the numerous benefits it offers, including fund transfers, checking account management, and bill payments [3].

HOW TO CITE:
Garba, J., Kaur, J., and Ibrahim, E. N. M. "Design of a Conceptual Framework for Cybersecurity Culture amongst Online Banking Users in Nigeria", *Nigerian Journal of Technology*, 2023; 42(3), pp. 399 – 305; https://doi.org/10.4314/njt.v42i3.13

However, alongside the immense advantages of online banking, the banking sector in Nigeria faces persistent cybersecurity challenges. Despite substantial investments in securing data, networks, and cyber defines systems, the occurrence of cybersecurity breaches and vulnerabilities is on the rise [4]. The prominence of human factors in contributing to these cybersecurity risks cannot be overlooked. Human behaviour and actions often introduce inconsistencies and errors, posing substantial threats to information assets. Consequently, a comprehensive understanding of the human factors that influence cybersecurity culture is essential for effective risk mitigation [5].

Cybersecurity culture is the collective mindset, attitudes, and behaviours of individuals, organizations, and society as a whole towards ensuring and promoting the security of digital systems and information. It encompasses a shared understanding of the importance of cybersecurity, a commitment to implementing best practices and protocols, and a proactive approach to identifying and mitigating cyber risks. A strong cybersecurity culture fosters a security-conscious environment where cybersecurity is integrated into daily practices and where individuals are vigilant and proactive in protecting against cyber threats [6].

While the significance of human factors in shaping cybersecurity culture has been recognized, there remain notable gaps in the existing literature. Specifically, limited research has been conducted to identify and explore the specific human factors influencing cybersecurity culture among online banking users in Nigeria. The available literature primarily focuses on assessing the state of cybersecurity in Nigeria, with insufficient attention given to cybersecurity culture, standards, interpersonal trust, and social norms. As a result, there is a pressing need to bridge this gap and develop a comprehensive conceptual model that addresses the unique Nigerian context [7].

This study aims to fill the gaps by providing a well-grounded conceptual model that identifies and examines the key human factors influencing cybersecurity culture among online banking users in Nigeria. This research will contribute to the enhancement of cybersecurity practices, risk mitigation, and the overall cybersecurity culture in the Nigerian online banking sector. The systematic literature review will serve as the foundation for developing a robust conceptual model that encompasses the identified human factors and their interrelationships. By distilling and analysing the literature, this research aims to provide valuable insights into the specific human factors influencing cybersecurity culture. The model will shed light on the complexities and dynamics of these factors, facilitating a comprehensive understanding of their impact on cybersecurity behaviour among online banking users.

Also, it is crucial to highlight the limitations of previous milestone works in this field [8-9]. Although previous works have contributed significantly to the understanding of cybersecurity culture and behaviour, their focus on developed countries with distinct demographic, cultural, and infrastructural settings raise questions about the universality of their findings. Moreover, the limited research conducted in Nigeria primarily focused on assessing the state of cybersecurity, rather than delving into the realm of cybersecurity culture. Therefore, this study seeks to rectify these limitations and contribute novel insights specific to the Nigerian context.

By addressing the gaps in the existing literature, this research endeavours to provide a comprehensive understanding of the human factors that influence cybersecurity culture among online banking users in Nigeria. The findings will serve as a foundation for designing targeted interventions, policies, and educational programs to promote responsible cybersecurity practices and mitigate cyber threats. Ultimately, the aim is to foster a strong cybersecurity culture that safeguards the interests of online banking users, protects sensitive information, and ensures the sustainable growth of online banking in Nigeria.

2.0 METHODOLOGY

The methodology employed for developing the conceptual model involved a systematic review of previous cybersecurity frameworks and research papers relevant to cybersecurity culture. This process aimed to identify and analyze the key factors influencing cybersecurity culture. The gathered literature underwent a qualitative content analysis, whereby relevant documents were identified and classified. This approach allowed for a systematic examination of the variables and constructs proposed in previous research within the cybersecurity culture domain.

3.0 CONCEPTUAL MODEL DEVELOPMEN-T

The development of a robust cybersecurity culture model requires consideration of existing frameworks in the field. A thorough review of previous cybersecurity frameworks was conducted, leading to

https://doi.org/10.4314/njt.v42i3.13

the formulation of the current conceptual model for cybersecurity culture. The primary objective of this comprehensive evaluation was to provide a comprehensive summary and analysis of variables proposed in previous researches within the cybersecurity culture domain, thereby supporting the conceptual model of the present study. Extensive literature searches were conducted across prominent digital databases, including Emerald, AIS, Elsevier Science Direct, ACM, Springer, and Google Scholar, focusing on papers published between 2018 and 2022 and employing keywords such as "Cybersecurity Culture" and "human factors." Through qualitative content analysis, relevant documents were identified and classified. In total, 44 papers specifically addressed Cybersecurity Culture, with 28 papers (representing 64% of the total) aligning with the Cybersecurity Culture framework, in line with the study's objectives. The remaining papers covered a range of topics, including definitions of cybersecurity culture, distinctions between organizational culture and national culture in relation to cybersecurity culture, strategies for developing national and organizational cybersecurity culture, and the goals of cybersecurity culture development.

Table 1: The Summary of key Human Factors.

Research	Constructs
[11]	Knowledge, assumptions, norm and value, artifact.
[12]	Management commitment to information security, security policy and policy enforcement, security Awareness, security training and education, security risk assessment, security compliance, ethical conduct.
[13]	Security compliance, top management, security, communication, job satisfaction.
[14]	Security behaviour, security awareness, social norm, enforcement of information security policy.
[15]	Security policy, SETA program and Security monitority.
[16]	**Organizational level:** Assets, continuity, trust, operations, defense, security governance. **Individual level:** Awareness, attitude, behaviour, competency.
[17]	**Organizational culture model:** Cybersecurity culture has three layers: **Corporate Politics:** Cybersecurity policy, organizational structure, resources. **Management:** Implementation of cybersecurity policy, benchmarks, responsibilities, qualification, and training. **Individual:** Attitude, communication, and compliance.
[18]	Knowledge, education, awareness, risk management, monitoring, compliance, normative value.
[19]	**Top Management Security,** Security Policy, security education and Training, security awareness, **Security Ownership,** Security risk analysis and assessment, ethical conduct, security compliance.
[20]	Security awareness, security knowledge, top management security policy security education security compliance, trust, norms.
[21]	**Organizational level:** Policy and procedure, risk analysis, budget, benchmarking. **Group level:** Management, interpersonal trust. **Individual:** Awareness, ethical conduct.
[22]	**Managerial:** Policy and procedures, risk analysis, budget, response, **Behavioural:** Responsibility, integrity, trust, norm and value, orientation, motivation **Individual:** Training, education, awareness
[23]	**Top Management.** Information security policy, information security awareness and education, information security behaviour, information security acceptance
[24]	Management support, communication, cybersecurity knowledge, cybersecurity awareness cybersecurity guideline
[25]	External environmental factors, national culture (social norm), political and legal factors, economic factors, socio-cultural factors, technical and technological factors, management factors, management and governance, information security policies and procedure, cybersecurity risk management, security education training, awareness and communication, cybersecurity behaviour, knowldege of cybersecurity, cybersecurity compliance
[26]	Security knowledge, security policy, security awareness
[27]	Trust, social norm, cybersecurity compliance, cybersecurity knowledge, cybersecurity awareness, cybersecurity eduaction

Table 1 summarizes the list of previous cybersecurity culture research constructs for each study. The first column of the Table 1 represents various cybersecurity culture research frameworks. The second columns represent constructs and findings for each relative cybersecurity culture frameworks.

Eighteen studies were retrieved in Table 1. The process used to develop the conceptual model was to extract research in existing information security culture frameworks and models in order to develop an understanding of current information security culture phenomena. For each study, all the proposed constructs were extracted and counted in Table 2. The purpose for counting constructs for each study is to identify top constructs as potential candidates because it is simply impossible to examine every factor that could help conceptualize a security culture. Because of the scope limitation, the current paper will only consider the top constructs where there is strong agreement between academic researchers as to their importance for cybersecurity culture. Table 2 presents top key constructs for that influence cybersecurity culture among online banking users.

3.1 Scenario Design

In Table 1 above, the review of previous research and the adopted constructs from each study were analysed. The key constructs that influencing cybersecurity culture and led the development of conceptual model are summarized in Table 2. In the section that follows, we lay out the basic framework for modelling cybersecurity culture (see Figure. 1) and hypothesize about the link between cybersecurity cultures and influencing factors. Based on our review of the research, we selected the following top seven key variables as show below:

Table 2: Summary of the Key Constructs

Constructs	Number of cited	Ranking
Interpersonal trust	5	7
Social norms	7	4
Cybersecurity awareness	14	1
Cybersecurity education	9	3
Cybersecurity knowledge	7	4
Cybersecurity policy	11	2
Cybersecurity compliance	7	4

3.1.1 Justification for ranking of conceptual factors

To determine the ranking of key constructs that influence cybersecurity culture among online banking users, the proposed constructs from each study were counted and analyzed. The purpose of ranking was to identify the top constructs with strong consensus and importance among academic researchers. The ranking of key constructs was based on the frequency of their appearance in the reviewed literature and their recognized significance in influencing cybersecurity culture. The ranking of conceptual factors in the proposed cybersecurity culture framework was determined through a systematic and evidence-based approach. This ranking process aimed to identify the most influential factors based on their frequency in the reviewed literature and their recognized significance in shaping cybersecurity culture among online banking users in Nigeria.

Cybersecurity Awareness (Ranked 1): The top ranking of "cybersecurity awareness" is grounded in its consistent and prominent emphasis in the reviewed literature. Multiple studies and academic research papers consistently underscored the critical role of cybersecurity awareness in cultivating a security-conscious mindset among online banking users. It emerged as the most frequently cited and emphasized factor across the selected literature, signifying its central importance in influencing cybersecurity culture.

Cybersecurity Policy (Ranked 2): "Cybersecurity policy" secured the second position due to its recognized significance in guiding and enforcing cybersecurity practices. Numerous studies highlighted the importance of well-defined policies in setting the foundation for cybersecurity culture. It was consistently cited and emphasized in the literature as a pivotal factor in promoting security-conscious behavior.

Cybersecurity Education (Ranked 3): "Cybersecurity education" claimed the third rank based on its crucial role in equipping online banking users with the knowledge and skills needed to navigate the digital landscape securely. While slightly less frequent than awareness and policy, education was consistently recognized as a fundamental factor in enhancing cybersecurity culture.

The ranking reflects the prevalence and importance of each construct as evidenced by the reviewed literature. Notably, “cybersecurity awareness” emerged as the top-ranked factor due to its consistent emphasis and recognition in the field, highlighting its central role in shaping cybersecurity culture.

This approach ensures transparency and objectivity in the development of the conceptual model, as the ranking is grounded in a systematic review of existing research rather than subjective opinions.

3.2 Conceptual Model

The conceptual model human factors that influencing cybersecurity culture among online banking users in Nigeria.

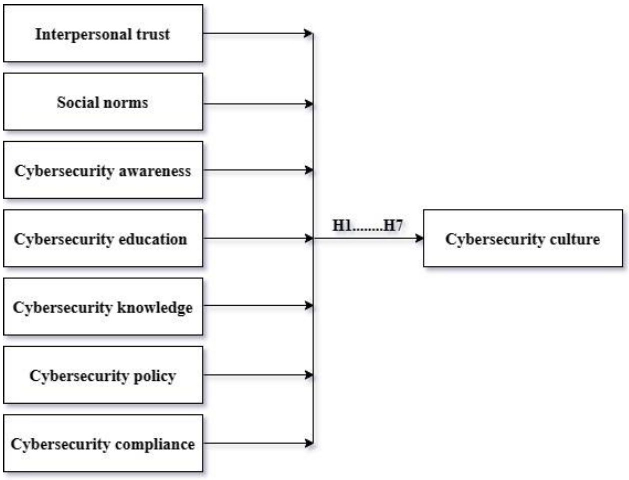

Figure 1: Conceptual Model

3.3 Hypotheses

Based on Figure 1, we can hypothesize the followings:

1- H1: Interpersonal trust significantly influences cybersecurity culture.

2- H2: Social norms significantly influence cybersecurity culture

3- H3: Cybersecurity awareness significantly influence cybersecurity culture

4- H4: Cybersecurity education significantly influence cybersecurity culture

5- H5: Cybersecurity knowledge significantly influence cybersecurity culture

6- H6: Cybersecurity policy significantly influence cybersecurity culture.

7- H7: Cybersecurity compliance significantly influence cybersecurity culture.

4.0 DISCUSSION

The existing literature review provides and highlighted the key human factors that influence the Cybersecurity Culture among Nigerian internet banking customers. The significance and effectiveness of these human factors on Cybersecurity Culture are vary. From the Table 1 for the summary of previous research on cybersecurity culture the cybersecurity awareness, cybersecurity education and cybersecurity policy are the most construct proposed by the researchers. all of this clearly shows that cybersecurity awareness, education, and policy are the most important factors in identifying the value of cybersecurity, as they work to develop a strategic framework to educate users of the need to follow the cybersecurity policy to avoid any cybersecurity incidents and to enhance the security of users by minimizing the possible cyberthreat.

However, the culture of cybersecurity must be strengthened according to strategic plans and scientific methodology, in addition to educating everyone on the necessity and importance of awareness of the concept of cybersecurity culture and exchanging experiences in this regard. Furthermore, the literature review reveals that there is a lack of investigation into what is required of Cybersecurity knowledge that should be incorporated across the organization and individuals to improve Cybersecurity culture. Furthermore, the review also found that very few researchers have addressed the influence of social influence and interpersonal trust on cybersecurity culture. The review also suggested that having an effective cybersecurity culture may potentially contribute to positive cybersecurity behavior, there is a considerable research gap in recognizing each variable and assessing its influences on Cybersecurity culture among organization and individual.

In comparing the findings of this study with recent and related published reports, several commonalities and variations can be observed. Firstly, the importance of cybersecurity awareness, education, and policy as influential factors in cybersecurity culture is consistent across multiple studies. These factors are consistently recognized as essential for promoting a security-conscious mindset and behavior among online banking users in Nigeria.

However, it is worth noting that while cybersecurity awareness, education, and policy are widely acknowledged, the specific strategies and approaches for implementing them may differ among studies. Some reports emphasize the role of awareness campaigns and training programs, while others focus on the development and enforcement of robust cybersecurity policies. These variations highlight the need for tailored approaches that consider the unique context and characteristics of online banking users in Nigeria.

Another notable finding from this study, which aligns with some published reports, is the lack of comprehensive investigation into the required cybersecurity knowledge across organizations and individuals. While the importance of cybersecurity knowledge is acknowledged, there is a research gap in understanding the specific knowledge areas that should be prioritized and incorporated into cybersecurity culture initiatives.

Additionally, this study highlights the limited attention given to social influence and interpersonal trust as factors influencing cybersecurity culture. Similarly, some recent reports also identify this gap, emphasizing the need to explore the role of social dynamics and trust relationships in shaping individuals' cybersecurity behaviours and attitudes.

5.0 CONCLUSION

To conclude, this study provides valuable insights into the human factors influencing cybersecurity culture among online banking users in Nigeria. Through a comprehensive review of existing literature, several key findings have emerged, highlighting the significance of cybersecurity awareness, education, and policy in fostering a secure online banking environment. The findings emphasize the need for strategic initiatives to enhance cybersecurity culture in Nigeria. By prioritizing cybersecurity awareness campaigns, implementing comprehensive educational programs, and developing robust policies, financial institutions and relevant stakeholders can empower online banking users with the knowledge and skills needed to protect themselves against cyber threats. Furthermore, the study highlights the importance of recognizing and addressing the specific cybersecurity knowledge requirements across organizations and individuals. Efforts should be made to identify and incorporate relevant knowledge areas into training programs and organizational practices, ensuring a comprehensive understanding of cybersecurity principles and practices. The study also emphasizes the role of social influence and interpersonal trust in shaping cybersecurity culture. Recognizing the impact of social dynamics on individual behaviours and attitudes, it is essential to foster a supportive and collaborative environment that encourages responsible cybersecurity practices.

Moving forward, it is recommended that further research be conducted to explore the identified research gaps and expand the understanding of cybersecurity culture in the Nigerian online banking context. This includes investigating the effectiveness of different awareness strategies, evaluating the impact of specific cybersecurity knowledge areas, and exploring the dynamics of social influence and trust in shaping cybersecurity behaviours. In conclusion, by implementing the insights gained from this study and adopting a proactive approach to cybersecurity culture, Nigeria's online banking sector can strengthen its resilience against cyber threats and create a safer digital environment for all users.

REFERENCES

[1] Alshaikh, M. "Computers and Security Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective", *computer and security 98*, 2020.

[2] Wong, W. P., Hwee, C. T., Kim, H. T., and Ming, L. T. "Human Factors in Information Leakage: Mitigation Strategies for Information Sharing Integrity", *Industrial Management and Data Systems*, 119(6): 1242–67, 2019.

[3] Chowdhury, N. H., Marc, T. P., Adam, and Timm, T. "Time Pressure in Human Cybersecurity Behavior: Theoretical Framewo-rk and Countermeasures", *Computers & Security 97*: 101963; 2020.

[4] Conteh, N. Y., and Paul, J. S. "Cybersecurity: Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks", *International Journal of Advanced Computer Research* 6(23): 31–38; 2016.

[5] Kathryn, P., Butavicius, M., Delfabbro, P., and Lillie, M. "Predicting Susceptibility to Social Influence in Phishing Emails", *International Journal of Human-Computer Studies*, 128: 17–26; 2019. https://doi.org/10.1016/j.ijhcs.2019.02.007

[6] Karen, L., and Schneier, B. "Privacy Threats in Intimate Relationships", *Journal of Cybersecurity* 6(1): 1–13; 2020.

[7] Uchendu, B., Jason R. C., Nurse, Maria B., and Furnell, S. "Developing a Cyber Security Culture: Current Practices and Future Needs", *Computers and Security 109*, 2021.

[8] Muhamad, R., and Padjadjaran, U. "Cybersecurity Policy and Its Implementation in Indonesia", *Journal of ASEAN Studies*, 2019.

[9] Orehek, Š., and Gregor, P. "A Systematic Review of Scales for Measuring Information Security Culture", *Information & Computer Security*, 2020.

[10] Hallikainen, H., and Laukkanen, T. 2018. "National Culture and Consumer Trust in E-Commerce", *International Journal of Information Management*, 38(1): 97–106; 2018. http://dx.doi.org/10.1016/j.ijinfomgt.2017.07.002

[11] Ameen, N. et al. "A Cyber Security Awareness and Education Framework for South Africa", Journal of Physics: Conference Series 51(14): 103284, 2020. https://doi.org/10.1016/j.im.2020.103284%0Ahttps://doi.org/10.1016/j.tele.2020.101415%0Ahttps://doi.org/10.1016/j.ijinfomgt.2020.102123%0Ahttps://doi.org/10.1016/j.chb.2020.106531

[12] Griggio, C. F., Nouwens, M., McGrenere, J., and Mackay, W. E. 2019. "Augmenting Couples' Communication with Lifelines: Shared Timelines of Mixed Contextual Information", *Conference on Human Factors in Computing Systems – Proceedings*, 2019.

[13] Inegbedion, H. E. 2018. "Factors That Influence Customers' Attitude toward Electronic Banking in Nigeria", *Journal of Internet Commerce*, 17(4): 325–38; 2018. https://doi.org/10.1080/15332861.2018.1463482

[14] Huang, K., and Pearlson, K. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture", *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019; For 6398–6407

[15] Georgiadou, A., Mouzakitis, S., Bounas, K., and Askounis, D. "A Cyber-Security Culture Framework for Assessing Organization Readiness", *Journal of Computer Information Systems*, 00(00), 1–11; 2020. https://doi.org/10.1080/08874417.2020.1845583

[16] Sarjiyus, O., Oye, N. D., and Baha, B. Y. "Improved Online Security Framework for E-Banking Services in Nigeria: A Real-World

Perspective", *Journal of Scientific Research and Reports*, 23(1): 1–14; 2019.

[17] Nasir, A., Arshah, R. A., and Ab Hamid, M. R. "Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework", *ACM International Conference Proceeding Series*, Part F1282, 56–60; 2017. https://doi.org/10.1145/3077584.3077593

[18] Triplett, W. "Establishing a Cybersecurity Culture Organization." *Acta Scientific Computer Sciences*, 3(8): 44–49; 2021.

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

[20] Madugba, J. et al. "Effect of Electronic Banking on Financial Performance of Deposit Money Banks in Nigeria", *Banks and Bank Systems*, 16(3): 71–83, 2021.

[21] Gcaza, N. et al. "Cybersecurity Culture: An Ill-Defined Problem", *HAL open science* (May 2017): 98–109; 2018.

[22] Reegård, K. "The Concept of Cybersecurity Culture the Concept of Cybersecurity Culture", *Proceedings Ofthe 29th European Safety and Reliability Conference.*, 2019, October. https://doi.org/10.3850/978-981-11-2724-3

[23] Muhamad, R., and Padjadjaran, U. 2019. "Cybersecurity Policy and Its Implementation in Indonesia", *Journal of ASEAN Studies*, (February) 2019.

[24] Veiga, A. da, Astakhova, L. V., Botha, A., and Herselman, M. "Defining organisational information security culture – Perspectives from academia and industry", *Computers and Security*, 101713; 2020. https://doi.org/10.1016/j.cose.2020.101713

[25] Nasir, A., Journal, I., Nasir, A., Arshah, R. A., Rashid, M., Hamid, A., Fahmy, S., and Bakar, M. A. "Information Security Culture Model for Malaysian Organizations: A Review", *International Journal of Advanced Trends in Computer Science and Engineering*, 1, 2020;

[26] Ocloo, C. M., da Veiga, A., and Kroeze, J. (2021). "A Conceptual Information Security Culture Framework for Higher Learning Institutions", *IFIP Advances in Information and Communication Technology*, 613, 63–80; 2021. https://doi.org/10.1007/978-3-030-81111-2_6