Cyber4Dev Security Culture Model for African Countries

Victor Reppoh[1,2] [0000-0002-5687-3447] and Adéle da Veiga[1] [0000-0001-9777-8721]

[1] School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South Africa
[2] Information Technology Management (ITM) World Health Organization – Zimbabwe, Harare, Zimbabwe
reppohv@who.int; dveiga@unisa.ac.za

Abstract. Creating a good information security culture among employees within organizations is the cornerstone for a safe and robust cyberspace. Furthermore, a strong information security culture within organizations will assist in reducing the effects of human habits that lead to data breaches. This article seeks to conduct a scoping review of the scholarly literature on Cyber Resilience for Development (Cyber4Dev) security culture within the context of African countries. With limited scholarly articles available for Cyber4Dev, the review will focus on information security culture to adapt it to a Cyber4Dev security culture that organizations in Africa can replicate. Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) for the scoping review, this paper analysed 40 scholarly articles on information security culture to propose a Cyber4Dev security culture model for organizations applicable within an African context. Economic, social-culture and trust were identified as some of the factors to consider in an African context to promote an information security culture. Organisations can consider these factors as part of their information security programs. The model serves as reference for further research to explore the influence of the identified factors in an African context.

Keywords: information security culture; Cyber4Dev; cyber security, cyber resilience, developing

1 Introduction

With the rapid expansion of the internet and its dependent technologies like cloud computing, cyber security threats have also grown exponentially [1]. Developing countries, especially those in Africa, are highly susceptible to these threats due to a myriad of challenges, including inadequate technological infrastructure, low literacy rates, and poverty, which harm cyber security awareness. As a result, Africa is a soft target for cybercriminals [2]. With these pitfalls in mind, Cyber Resilience for Development (Cyber4Dev), a European Union project, seeks to ensure that developing countries enjoy a digital environment that is open, irrepressible, and secure [3]. Unfortunately, under the African Union (AU) banner, African countries have not fully complied with their own African Union Convention on Cyber Security and Personal Data Protection due to innumerable challenges faced on the continent [4].

This paper seeks to conduct a scoping literature review of the scholarly literature on Cyber Resilience for Development (Cyber4Dev) security culture within the context of African countries. The Cyber4Dev project is a relatively new concept and thus still has limited available literature. Therefore, the authors reviewed the literature on the broad concept of information security culture with a bias towards African countries due to their unique governance, poverty, infrastructure, and literacy challenges, which hamper efficient and effective cyber security culture development [5]. The authors reviewed and consolidated information from 40 articles on information security culture and proposed a Cyber4Dev Security Culture Model for use by organizations in Africa.

2 Research problem and research questions

Cyber4Dev security culture is a new concept with very little scholarly literature available for review or study. Consequently, research material on this European Union project is scarce with its website positing its objective for international cooperation to bring about adequate capacity in cyber security [6]. However, many scholarly articles on information security culture need contextualizing into an African perspective. With their litany of difficulties curbing cybercrimes, including inadequate legal frameworks, technological inadequacies, lack of requisite human resource skills and security, African countries have unique information security challenges [7]. Many African internet users are not technically skilled, with a large percentage of them having restricted access to computers and the internet [8]. In Mozambique, for example, there is a scarcity of cyber security awareness programs, skills development, and cyber security training and education [8]. In Gambia by September 2020, there were no national cybersecurity awareness programs initiated by the government to raise awareness on the pitfalls of insecure cyberspace practices [9]. Even though South Africa is one of the few African countries having a national cybersecurity policy framework addressing the cybersecurity environment, little is known about this policy and information on safeguarding cyberspace [9]. Literature on information security culture is abounding, but there is limited focus to adapt and implement it in an African context.

This paper aims to define Cyber4Dev security culture from an African perspective and contribute to this area's limited body of knowledge. In line with achieving this objective, the author formulated the following research questions:

- Which are the models or frameworks developed for the Cyber4Dev security culture?
- What factors should be considered when creating a Cyber4Dev security culture model?

3 Background

3.1 Defining Information Security Culture and Cyber4Dev Security Culture

The assumptions, ethics, and attitudes that employees share about the safety of institutional data are defined as the information security culture. This culture is a sub-culture of the organizational culture that encompasses the employees' everyday responsibilities, guidelines, activities, and practices that should assist them in protecting the firm's information assets [9]. The rapid development of new technologies in the information and communication technology (ICT) industry has also led to exponential growth in information security risks [10]. Information security culture helps to secure security risks within organizations by promoting safe cyber practices by individuals [11][12]. However, more researchers have posited that solving information security risks and threats cannot purely be from a technological perspective [13]. Human capital plays a crucial role in securing organizations from these cyber threats; humans being viewed as the weakest link in information security terms [13][14]. Any institutional interventions to curb cyber threats or risks which fail to consider the human element dismally fall short of the requisite expectations [15]. Employees, for example, need to act and manipulate institutional information in a consistent manner compliant with the organization’s information security policy [16]. Social and national cultures like obedience to authority, can impact an individual's attitudes and assumptions, and thus shape an information security culture [17]. Furthermore, information security culture is dynamic and ever-changing, and thus, a balance between stability and constant evolution is needed to ensure that organizations adequately protect their information systems.

Cybersecurity culture is a subset of information security culture that describes how users protect data in cyberspace. On the other hand, the entire lifecycle of information (in its various formats) within organizations, as well as the safeguards that users employ to protect it, is the focus of an information security culture [18]. A Cyber4Dev security culture likewise can be defined as people-driven, cyber-safe actions and behaviors that protect organizations’ information assets in developing countries. This culture takes cognizance of the shared assumptions, ethics, and attitudes, of employees in African organizations towards the protection information assets. Adopting a Cyber4Dev security culture will ensure that employee interactions with information resources will not harm the institutions via the information superhighway [19]. Employees, when adequately trained, can become an organization’s most vital link when it comes to the security of information resources [20]. A Cyber4Dev security culture will ensure that individuals within African organizations make accountable decisions and take responsible actions that safeguard organizations’ information assets.

3.2 Cyber Security Challenges in Africa

The term "cyber security" refers to the protection of computer systems from theft, damage, or manipulation of their hardware, software, or data. In Africa, technology adoption is increasing at an exponential rate, with mobile smart device ownership, social media usage, and the Internet of Things (IoT) becoming a reality. Even the most pessimistic data suggest that Africa is on course to make considerable progress and contribute to global growth. However, with increased affluence come new dangers and vulnerabilities that may jeopardize development [21]. Africa is exposed to cyber threats and possible harms due to limitless cyberspace, which does not recognize borders, inadequate information security funding, and weak legislation [22]. Therefore, information security is a critical economic and national security concern that requires careful definition and context. According to the United Nations Economic Commission for Africa [23], and various surveys, Africa is vulnerable to cyberthreats because of its many domains and poor network and information security. According to estimates, cybercrime costs the African economy $895 million each year [24][25].

Many developing countries lack the resources and capabilities of industrialized countries, making cyber security a major concern for businesses in sub-Saharan Africa. [22]. In many African countries, cyber security is still seen as a luxury rather than a need with firms' cyber security budgets being less than 1%, and many organizations have no cyber security budget at all according to the World Bank's 2016/17 Global Cybersecurity Report [8]. There is a low rate of Information Communication Technology (ICT) literacy [26]. As a result, ICT users in Africa are inexperienced and technologically illiterate. Most are also illiterate in English, which is critical because most security product information is only in English [8]. In addition, basic requirements such as housing, food, health, and education frequently take precedence over the adoption of ICT [27].

3.3 Cyber Awareness in Africa

Cyber awareness is described as employees' understanding toward the security of the organization's information assets. Being security-conscious entails being aware of the risks associated with an organization's information assets and how to protect them [28]. Unfortunately, the lack of understanding within Africa about the risks of accessing cyberspace contributes to a permissive climate for cybercrime. African countries' digital infrastructure development level harms their security position, with cybercriminals taking advantage of poor security habits [29]. The significance of information security awareness in reducing the risks associated with data security breaches cannot be overstated [30]. Policymakers need to develop strong legislation and awareness programs to stem the rising flood of cyber risks in Africa [31]. Several organizations, like the African Information Society Initiative (UNECA/AISI), have previously emphasized the importance of continental collaboration and increased cyber security awareness [26].

3.4 Why Promote a Cyber4Dev Security Culture?

According to the Ernest and Young Global Information Security Survey (GISS) [32], the number of damaging attacks against organizations increased dramatically during 2019, with 59 percent of them reporting severe security breaches. In addition, the number of employee error-related breaches increased six-fold [33]. Africa could benefit immensely from guidelines to promote a security culture that is adaptable to the

African context. A Cyber4Dev security culture would encourage governments, employees, and individuals to take the lead in combating cyber-security threats through awareness-raising, legislation, and performing cyber-safe practices. This paper will focus on Cyber4Dev security culture in Africa, a continent with a population with insufficient cyber skills, limited security awareness, inadequate infrastructure, and few training institutions that focus on cyber awareness[34].

4 Research Method

Scoping reviews give a broad overview of a specific topic without much regard for the quality of the study [35]. This paper utilizes the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method [35]. This methodology has two components, namely a systematic review and a meta-analysis. Its main objective is to ensure that literature reviews are conducted transparently and produce repeatable results [21].

4.1 Information Sources

The author selected four electronic databases. Each database had unique filtering tools to screen the large number of papers obtained from the initial search. Table 1 lists the databases and search strings (keywords) used in each for the initial broad searches conducted by the author.

Table 1. Search strings that were used in each database.

Database	Search String (Keywords)
Association of Computing Machinery (ACM)	[[[Abstract: security] AND [Abstract: information] AND [Abstract: security] AND [Abstract: culture]]] AND [[[Publication Title: security] AND [Publication Title: culture]]] AND [[[Full Text: security] AND [Full Text: culture]] OR [[Full text: information] AND [Full Text: security] AND [Full text: security] AND [Full Text: culture]] OR [[Ful Text: information] AND [Full text: security] AND [Full Text: culture]]] AND [Publication Date: (01/01/2015 TO 08/31/2021)]
Electrical and Electronic Engineers (IEEE)	("Document Title”: security AND "Document Title”: Culture OR "Document Title”: Information AND "Document Title”: Security AND "Document Title”: Culture) OR ("Abstract”: security AND "Abstract”: Culture OR "Abstract”: Information AND "Abstract”: Security AND "Abstract”: Culture) OR ("Index Terms”: Security AND "Index Terms”: Culture OR "Index Terms”: Information AND "Index Terms”: Security AND "Index Terms”: Culture)
Scopus	TITLE-ABS-KEY (security AND culture OR information AND security AND culture) AND (LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (OR LIMIT-TO (PUBYEAR, 2016) OR LIMIT-TO (PUBYEAR, 2015)) AND (LIMIT-TO (SUBAREA, "COMP")) AND (LIMIT-TO (LANGUAGE, "English"))
Web of Science	((((TS= (Security AND Culture OR Information AND Security AND Culture)) AND AB= (Security AND Culture OR Information AND Security And Culture)) AND TI= (Security AND Culture OR Information AND Security And Culture)) AND PY= (2015 OR 2016 OR 2017 OR 2018 OR 2019 OR 2020 or 2021)) AND AK= (Security AND Culture OR Information AND Security And Culture)

4.2 Eligibility Criteria

The articles had to meet specific criteria. Firstly, all papers should be from published journals and conference papers. Secondly, the papers should be written in English between 2015 and 2021. Thirdly, the subject areas were limited to Computer Science and Engineering, and finally, the country/regions were restricted to countries in Africa.

4.3 Data Collection

After searching within the databases, the article title, article abstract, author name(s), the journal name, keywords, and the publication year of the identified articles then exported as a CSV file into a Microsoft Excel spreadsheet; the authors then screened the selected papers by going through the article abstracts and keywords. From the 925 articles retrieved from the databases, 797 were discarded based on abstract review and duplicate removal. After a full text review of the articles a further 88 articles were discarded leaving 40 articles used in this study.

5 Results

5.1 Synthesis of the Results

Of the chosen articles, twenty-one (21) were journal articles and nineteen (19) were from conference papers. Many of these articles were published in 2015 (14) with the least number published in 2018 (3) and 2020 (3). The summary of the publication types and the year in which the papers were published is represented in table 2.

Table 2. Summary of publication types and years they were published.

	2015	2016	2017	2018	2019	2020	2021
Journals	5	2	2	2	4	2	4
Conference Papers	9	2	3	1	3	1	0

The bulk of the analyzed articles (29) had a clear definition of information security culture or security culture. The rest of the papers (11) did not give a definitive definition for either security culture or information security culture although the terms were used copiously within the articles. In summary, a Cyber4Dev security culture was defined as people-driven, cyber-safe activities and behaviors that protect developing-country organizations' information assets. The definition highlighted the important role of people in the success of an information security culture within African organizations.

Most publications (28) examined created conceptual models or based their studies on a specific framework or model. The Information Security Culture Framework (ISCF) (7) [36], [37], [38], [39], [40], [41], [42], was the most often used or altered framework/model in the publications reviewed. Other identified models included the Organizational Security Culture Model [43], Information Security Shared Tacit Espoused Values (MISSTEV) model [44] [45], STOPE (Strategy; Technology; Organization; People; and Environment) Framework [10], and the TOE (Technology, Organization, and Environment) model [46]. The bulk of publications (32) included information security cultural factors. Table 3 summarizes the factors considered vital in developing an information security culture from these articles. Only factors with more than 10 citations were included.

Table 3. Important information security culture factors.

Factors	Total	Papers
Information security training	10	[47], [36], [48],[49], [12], [38], [44], [50], [15], [16]
Compliance and trust	11	[47],[36],[48],[51],[12],[52],[37],[46],[39],[43],[41]
Information security policy/regulations	16	[47], [36], [48], [51], [49], [52], [37], [46], [38], [21], [10], [53], [41], [45], [15], [11]
Top management/leadership support	18	[47], [36], [48], [51], [49], [52], [37], [46], [38], [21], [54], [39], [10], [43], [55], [15], [11], [56]
Information security awareness and sharing	20	[47], [36],P4, [49], [52], [37], [46], [38], [21], [54], [39], [44], [53], [55], [41], [45], [11], [15], [16], [56]

Employees gain information security knowledge and skills they need to navigate cyberspace through information security training. Information security policies guide the security culture within organizations and direct employee behavior for compliance with information security policies. Compliance and by-in to these policies promote a positive information security culture [37]. Top management defines the strategies that ensure a cyber-secure work environment. These factors are also relevant to African countries as they form the pillars in successfully implementation of cyber-safe practices within organizations and thus are utilized in the proposed Cyber4Dev Security Culture Model.

5.2 The African Perspective

In total, thirteen papers [11], [16], [20], [38], [44], [50], [51], [37], [46], [41], [45], [57], [58] were retrieved with an African perspective. Information security training (8) was the most significant component influencing a healthy information security culture in African organizations, which is in line with the work of the African Information Society and other related organisation's who emphasized the importance of information security training [26]. African organizations can utilize information security training to avoid and mitigate user risk by helping users and employees understand their role in preventing and mitigating information security breaches [15], whilst also ensuring that it is presented in African languages. Information security policy/regulations (7) are a set of rules and standards that govern the usage, management, and protection of information technology assets and resources [49]. African countries fall short in cyber-safe policy formulation and implementation thus exposing organizations to innumerable cyber threats. Economic (3), technological (3), and social-cultural/environmental (3) factors were prominently highlighted by African authors. Economic factors refer to financial/monetary conditions within these African countries that affect the organizations' ability to implement effective information security practices. The technology factors in the context of Africa encompass the numerous infrastructural and technical requirements for the effective protection of organizational information assets. The social-cultural and environmental factors are the forces inside societies that shape people's views, beliefs, and behaviors. These influences have a bearing on how individuals perceive the importance of cyber-safe practices and organizational information assets. Table 4, summarizes the main factors affecting African organizations in instilling good information security cultures.

Table 4. Important information security culture factors from an African perspective.

Factors	Total	Papers
Information security training	8	[11], [38], [44], [50],[51], [37], [41], [45]
Information security policy/regulations	7	[14], [16], [38], [51],[37], [41], [45],
Economic factors	3	[44], [51], [37]
Technological factors	3	[51], [37], [46]
Social-cultural / environmental factors	3	[44], [51], [46]

6 Cyber4Dev Security Culture Model

From the analysis of the thirteen (13) papers written by African authors or with an African perspective on information security culture, five factors were identified as the most influential to instilling a good information security culture within organizations in Africa, derived from table 4. Compliance and trust, top management support and information security awareness and sharing factors from table 3 were also incorporated to define the proposed model. Figure 1 depicts the proposed Cyber4Dev Security Culture Model, with the eight factors. According to the model, the information security culture influencing factors on the left and right have a beneficial impact on instituting an information security culture within organizations in Africa. Information security training, information security awareness and sharing, information security policy and regulations, and top management support (factors on the right) were most influential according to authors, in promoting an ideal information security culture in organizations. The interplay of these eight components can contribute to foster an information security culture that could be of benefit to African countries.

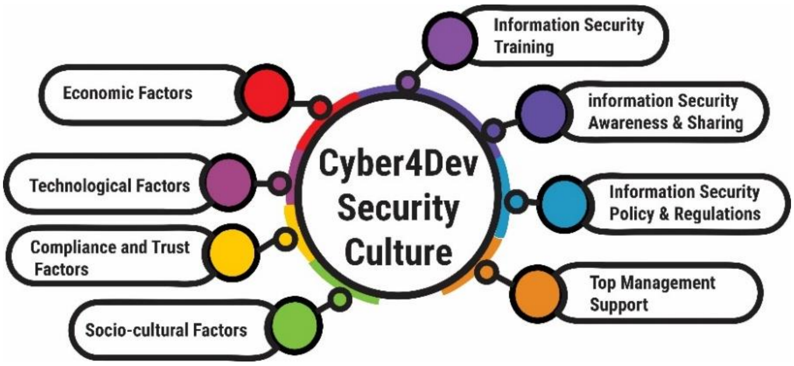
Cyber4Dev Security Culture
Economic Factors
Technological Factors
Compliance and Trust Factors
Socio-cultural Factors
Information Security Training
information Security Awareness & Sharing
Information Security Policy & Regulations
Top Management Support

Fig. 1. The Cyber4Dev Security Culture Model

The first request question aimed to identify existing models of frameworks for Cyber4Dev security culture, which was found to be lacking based on the literature review. Figure 1 answers the second research question by proposing a Cyber4Dev security culture model, being a novel model in the cyber for development context. Organisations can consider these factors as part of their information security programs and governments can incorporate it in their cyber resilience programs. The model serves as reference for further research to explore the influence of the identified factors in an African context.

7 Conclusion and future work

The Cyber4Dev Security Culture Model proposed in this paper provides a foundation for African countries and organizations to build a successful information security culture to secure information assets. The model's application to any African business would enhance its employees' awareness of and interactions with information assets, resulting in a positive impact and protection against numerous information security dangers posed by insiders. A Cyber4Dev security culture would encourage governments, employees, and individuals to take the lead in combating information security threats through awareness-raising, legislation, and performing cyber-safe practices. A limitation of the study is that the model is conceptual. Future work will aim to validate the model with cyber security experts from Africa using a qualitative method and to further expand the model for implementation as part of a case study to test it. Furthermore in future work the literature review could cover more than the five year period covered in this paper and include other domains in information security culture.

References

1. Sas, M., Hardyns, W., van Nunen, K., Reniers, G., Ponnet, K.: Measuring the security culture in organizations: a systematic overview of existing tools, (2021)
2. Kurebwa, J., Magumise, E.: The Effectiveness of Cyber Security Frameworks in Combating Terrorism in Zimbabwe. Int. J. Cyber Res. Educ. 2, 1–16 (2019). https://doi.org/10.4018/ijcre.2020010101
3. Cyber4Dev: Project objectives – Cyber4d – Cyber Resilience for Development, https://cyber4dev.eu/project-activities/
4. Abdulrauf, L.A.: Giving ‘teeth’ to the African Union towards advancing compliance with data privacy norms. Inf. Commun. Technol. Law. 30, 87–107 (2021). https://doi.org/10.1080/13600834.2021.1849953
5. Obuhuma, J., Zivuku, S.: Social Engineering Based Cyber-Attacks in Kenya. 2020 IST-Africa Conf. IST-Africa 2020. 1–9 (2020)
6. Campbell, M.: What’s in a project name? - Cyber Resilience for Development [Cyber4Dev], (2019)
7. ITU: Global Cybersecurity Index, 2017. ITU Publications (2019)
8. Kshetri, N.: Cybercrime and Cybersecurity in Africa. J. Glob. Inf. Technol. Manag. 22, 77–81 (2019). https://doi.org/10.1080/1097198X.2019.1603527
9. Nagyfejeo, E., Solms, B. Von: Why Do National Cybersecurity Awareness

Programmes Often Fail? Int. J. Inf. Secur. Cybercrime. 9, 18–27 (2020). https://doi.org/10.19107/ijisc.2020.02.03

10. Alhogail, A.: Design and validation of information security culture framework. Comput. Human Behav. 49, 567–575 (2015). https://doi.org/10.1016/j.chb.2015.03.054
11. Da Veiga, A., Martins, N.: Information security culture and information protection culture: A validated assessment instrument. Comput. Law Secur. Rev. 31, 243–256 (2015). https://doi.org/10.1016/j.clsr.2015.01.005
12. Nasir, A., Arshah, R.A., Hamid, M.R.A., Fahmy, S.: An analysis on the dimensions of information security culture concept: A review. J. Inf. Secur. Appl. 44, 12–22 (2019). https://doi.org/10.1016/j.jisa.2018.11.003
13. Orehek, Š., Petrič, G.: A systematic review of scales for measuring information security culture. Inf. Comput. Secur. 29, 133–158 (2020). https://doi.org/10.1108/ICS-12-2019-0140
14. Da Veiga, A.: An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Inf. Comput. Secur. 26, 584–612 (2018). https://doi.org/10.1108/ICS-08-2017-0056
15. Alnatheer, M.A.: Information security culture critical success factors. Proc. - 12th Int. Conf. Inf. Technol. New Gener. ITNG 2015. 731–735 (2015). https://doi.org/10.1109/ITNG.2015.124
16. Da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. 49, 162–176 (2015). https://doi.org/10.1016/j.cose.2014.12.006
17. Connolly, L.Y., Lang, M., Wall, D.S.: Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. Inf. Syst. Manag. 36, 306–322 (2019). https://doi.org/10.1080/10580530.2019.1651113
18. Da Veiga, A.: Achieving a Security Culture. 72–100 (2019). https://doi.org/10.4018/978-1-5225-7847-5.ch005
19. Mousavi, M.Z., Kumar, S.: Analysis of key Factors for Organization Information Security. Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019. 514–518 (2019). https://doi.org/10.1109/COMITCon.2019.8862191
20. Nel, F., Drevin, L.: Key elements of an information security culture in organisations. Inf. Comput. Secur. 27, 146–164 (2019). https://doi.org/10.1108/ICS-12-2016-0095
21. Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.: A systematic literature review: Information security culture. Int. Conf. Res. Innov. Inf. Syst. ICRIIS. 1–6 (2017). https://doi.org/10.1109/ICRIIS.2017.8002442
22. Schia, N.N.: The cyber frontier and digital pitfalls in the Global South. Third World Q. 39, 821–837 (2018). https://doi.org/10.1080/01436597.2017.1408403
23. United Nations Economic Commission for Africa: Policy Brief Tackling the challenges of cybersecurity in Africa, www.economist.com/, (2014).
24. KnowBe4: African Cybersecurity Research Report. 1–8 (2019).
25. Check Point Research: Cyber Security Report 2020. Security. 7, 1–15 (2020).
26. Bada, M., von Solms, B., Agrafiotis, I.: Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. Third Int. Conf. Cyber-Technologies Cyber-Systems, CYBER 2018. 78–83 (2018).
27. Schelenz, L., Schopp, K.: Digitalization in Africa: Interdisciplinary Perspectives on Technology, Development, and Justice. Int. J. Digit. Soc. 9, 1412–1420 (2018). https://doi.org/10.20533/ijds.2040.2570.2018.0175
28. Amankwa, E., Loock, M., Kritzinger, E.: Enhancing information security education and awareness: Proposed characteristics for a model. 2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015. 72–77 (2016).

https://doi.org/10.1109/InfoSec.2015.7435509

29. Von Solms, B., Bada, M., Agrafiotis, I.: Reviewing National Cybersecurity Awareness for Users and Executives in Africa. Int. J. Adv. Secur. 12, 108–118 (2019).
30. Ndiege, J.R., Okello, G.: Towards information security savvy students in institutions of higher learning in Africa: A case of a university in Kenya. 2018 IST-Africa Week Conf. IST-Africa 2018. 1–8 (2018).
31. Devi, A.: Cyber Crime and Cyber Security: Trends in Africa. 160–171 (2017). https://doi.org/10.4018/978-1-5225-2154-9.ch011
32. EY: EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in? (2020).
33. Nathan, A.J., Scobell, A.: 2020 Data Breach Investigations Report. Verizon. (2020)
34. Malatji, M., Marnewick, A.L., von Solms, S.: Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. Sustain. 13, 1–33 (2021). https://doi.org/10.3390/su13010291
35. Tricco, A.C., Lillie, E., Zarin, W., O'Brien, K., Colquhoun, H., Kastner, M., Levac, D., Ng, C., Sharpe, J.P., Wilson, K., Kenny, M., Warren, R., Wilson, C., Stelfox, H.T., Straus, S.E.: A scoping review on the conduct and reporting of scoping reviews. BMC Med. Res. Methodol. 16, 1–10 (2016). https://doi.org/10.1186/s12874-016-0116-4
36. Tolah, A., Furnell, S.M., Papadaki, M.: An empirical analysis of the information security culture key factors framework. Comput. Secur. 108, 102354 (2021). https://doi.org/10.1016/j.cose.2021.102354
37. Woretaw, A., Lessa, L., Negash, S.: Factors hindering full-fledged information security in banking sector in Ethiopia: Emphasis on information security culture. 25th Am. Conf. Inf. Syst. AMCIS 2019. (2019).
38. da Veiga, A., Martins, N.: Defining and identifying dominant information security cultures and subcultures. Comput. Secur. 70, 72–94 (2017). https://doi.org/10.1016/j.cose.2017.05.002
39. Nasir, A., Arshah, R.A., Ab Hamid, M.R.: Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. ACM Int. Conf. Proceeding Ser. Part F1282, 56–60 (2017). https://doi.org/10.1145/3077584.3077593
40. Chen, Y., Ramamurthy, K., Wen, K.W.: Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Syst. 55, 11–19 (2015). https://doi.org/10.1080/08874417.2015.11645767
41. Martins, N., Da Veiga, A.: An Information security culture model validated with structural equation modelling. Proc. 9th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2015. 11–21 (2015).
42. Hogail, A. Al: Cultivating and assessing an organizational information security culture; an empirical study. Int. J. Secur. its Appl. 9, 163–178 (2015). https://doi.org/10.14257/ijsia.2015.9.7.15
43. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Investigating the formation of information security climate perceptions with social network analysis: A research proposal. Pacific Asia Conf. Inf. Syst. PACIS 2015 - Proc. (2015).
44. Da Veiga, A.: Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study. Inf. Comput. Secur. 24, 139–151 (2016). https://doi.org/10.1108/ICS-12-2015-0048
45. Da Veiga, A.: The influence of information security policies on information security culture: Illustrated through a case study. Proc. 9th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2015. 22–33 (2015).
46. Mokwetli, M., Zuva, T.: Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa. 2018 Int. Conf. Adv. Big Data, Comput. Data

Commun. Syst. icABCD 2018. (2018). https://doi.org/10.1109/ICABCD.2018.8465139

47. Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S.: Developing a cyber security culture: Current practices and future needs. Comput. Secur. 109, 102387 (2021). https://doi.org/10.1016/j.cose.2021.102387
48. Arbanas, K., Spremic, M., Zajdela Hrustek, N.: Holistic framework for evaluating and improving information security culture. Aslib J. Inf. Manag. 73, 699–719 (2021). https://doi.org/10.1108/AJIM-02-2021-0037
49. Mousavi, M.Z., Kumar, S.: Analysis of key Factors for Organization Information Security. Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019. 514–518 (2019). https://doi.org/10.1109/COMITCon.2019.8862191
50. Da Veiga, A.: An information security training and awareness approach (ISTAAP) to instil an information security-positive culture. Proc. 9th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2015. 95–107 (2015).
51. da Veiga, A., Astakhova, L. V., Botha, A., Herselman, M.: Defining organisational information security culture—Perspectives from academia and industry. Comput. Secur. 92, 101713 (2020). https://doi.org/10.1016/j.cose.2020.101713
52. Nasir, A., Abdullah Arshah, R., Ab Hamid, M.R.: A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. Inf. Secur. J. 28, 55–80 (2019). https://doi.org/10.1080/19393555.2019.1643956
53. Tang, A., Han, J., Chen, P.: A comparative analysis of architecture frameworks. Proc. - Asia-Pacific Softw. Eng. Conf. APSEC. 640–647 (2004). https://doi.org/10.1109/APSEC.2004.2
54. Hassan, N.H., Maarop, N., Ismail, Z., Abidin, W.Z.: Information security culture in health informatics environment: A qualitative approach. Int. Conf. Res. Innov. Inf. Syst. ICRIIS. 1–6 (2017). https://doi.org/10.1109/ICRIIS.2017.8002450
55. AlKalbani, A., Deng, H., Kam, B.: Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure, (2015).
56. Nasir, A., Arshah, R.A., Hamid, M.R.A.: Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study. 2020 6th IEEE Int. Conf. Inf. Manag. ICIM 2020. 205–209 (2020). https://doi.org/10.1109/ICIM49319.2020.244699
57. DaVeiga, A.: An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Inf. Comput. Secur. 26, 584–612 (2018). https://doi.org/10.1108/ICS-08-2017-0056
58. Govender, S., Kritzinger, E., Loock, M.: The influence of national culture on information security culture. 2016 IST-Africa Conf. IST-Africa 2016. 1–9 (2016). https://doi.org/10.1109/ISTAFRICA.2016.7530607