Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania

Zainab Ruhwanya, Jacques Ophoff

Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania

Zainab Ruhwanya[1][0000-0003-2339-7154] and Jacques Ophoff[2][0000-0003-0634-5248]

University of Cape Town, Cape Town, South Africa
[1]RHWZAI001@myuct.ac.za, [2]jacques.ophoff@uct.ac.za

Abstract. This study explores the status of information security culture (ISC) of small and medium-sized enterprises (SMEs) in sub-Saharan Africa (SSA) using Tanzania as a case. To assess the ISC of SMEs, measurement criteria from organizational and environmental dimensions were compiled from the literature. A combination of quantitative and qualitative methods was employed to collect data. The ISC dimensions were assessed using surveys collected using both paper and online sources, from 39 SMEs in the roundtable and five focus group discussions. The findings indicated lack of information security policy, absence of security education, training and awareness (SETA) programs, lack of human resource, poor risk assessment, and management and lack of national information security culture initiatives. These findings show the immaturity of ISC in SMEs in Tanzania. The results and implications of these findings suggest further research and intervention is necessary to institutionalize ISC in the SME environment.

Keywords: Information security culture, information security, security, culture, Small and Medium-sized Enterprises, Tanzania, Sub-Sahara Africa.

1 Introduction

Fifty-eight percent (58%) of small and medium-sized enterprises (SMEs) experienced security attacks and data breaches in 2018 [1]. In today's ever-increasing information security threats landscape, cultivating information security culture (ISC) within an organization is critical. Not surprisingly, researchers are concerned with understanding, promoting, and assessing ISC in organizations. In response to this concern, several ISC theoretical frameworks have been proposed [2]–[6]. However, prior research has been focusing on assessment of ISC of large organizations. An SME is recognized as different from a large organization by its size, culture, and shortage of human and financial resources [7]. The few studies about the assessment of holistic ISC of SMEs are from the developed world [3], and little is known about SMEs from sub-Saharan Africa (SSA). SMEs are a significant and an essential part of SSA countries' economy, and information security is a critical success factor [8] for any enterprise. Thus, any security attack on SMEs harms the economy. For instance, for an SME to recover from a security breach approximately US$955,429 to US$1,207,965 is required [9]. This high recovery cost threatens the existence of an SME especially those from the poorest parts of the world.

This study is motivated by limited empirical research on ISC of SMEs in sub-Saharan Africa, and the need to develop ISC strategies that are context specific for SSA.

The study aims to explore the status quo of ISC of SMEs in SSA using Tanzania as the case. We posit that for ISC one size does not always fit all due to the contextual and operational differences of the parent nations and organizations [10], [11]. We pose the following question: *What is the current state of the information security culture of small and medium-sized enterprises in Tanzania?*

The rest of this paper answers this question by presenting ISC dimensions to explain the status of the ISC in Tanzania. The following section discusses the background literature and presents a list of ISC dimensions for assessment. Next, the research methodology is presented. The analysis of the data and a discussion of the results follow. Finally, we present the conclusions of the study.

2 Literature review

2.1 Information security culture

Information security is defined as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" [12]. Information security's objective is to preserve the critical characteristics of information namely confidentiality, integrity, and availability (CIA) when information is in storage, processing, or transmission [12]. Information security involves people, technologies and processes, yet the majority of security experts and organizations tend to look at the security problems from the technology viewpoint and as the solution [13]. However, people are the weakest link in information security [13]. It is evident that a majority of security violations cases results from behavioral issues such as human errors, and employee negligence [13], [14]. Hence to manage people's problems; there is a need for cultivation of ISC in the organizations [15].

Information security culture is referred to as the subset of the organizational culture [8]. Organizational culture is developed; is taught to new members, is learned on how to relate to the environment [16], is transferred from one generation another [17], and is necessary for problem-solving [16], [18], and it changes with time [16] to meet organizational visions [8]. Straub et al [10] classified definitions of culture into three categories, as (i) shared value views (sense of what ought to be) example Hofstede's [17] (ii) outcomes-oriented (problem-solving) views like Schein's [16], [18] and (iii) as a way of being (unconscious view).

Many information security culture scholars except for [2], [19] are defining ISC based what it is composed of and not what it is to accomplish. We argue that it is essential to look at the ISC in a problem-solving viewpoint. A problem-solving view of culture looks at what ISC can accomplish in the organization [10]. The problem in the information security space is that an organization must survive from the external and internal threats. Hence information security culture must make it possible to cope with organizational problems of external adaptation (control external security threats and data breaches) and internal integration (have consensus for the acceptable security behaviors) [16].

Hence, in a holistic way we define information security culture as *"a patterned way of security-based thinking shared within an organization; based on values, as-*

sumptions, and beliefs, which influences the behaviors and actions of the individuals so that, information security becomes a natural aspect in the daily activities in the organization. This ISC is developed, learned and changes with time with the aim to protect information assets and preserve confidentiality, integrity, and availability of information and information systems resources so as meet to the core organization vision"[2],[19].

2.2 Information security culture assessment

The review of the literature indicates that there are various frameworks for the ISC assessment of an organization [2]–[6],[20]. The frameworks present different dimensions including internal (organizational) and external (environmental) factors. Organizational dimension includes top management support [2]-[6], information security policy & procedures (ISP) [2]–[6] , risk assessment & management [2], security education, training, & awareness (SETA) programs [2]–[6], technical and human resources [2]–[6]. Environmental dimension includes national security culture initiatives [3, 4], suppliers/vendors [3], and partner organizations. Despite differences among frameworks on the specific constructs and relationships, there are some convergences among them. Particularly on the importance of the constructs such as top management support, ISP, and SETA programs and national security culture initiatives [3], which has been reported to have a positive influence on information security culture of an organization [21].

Although [2], [4]–[6], [20] frameworks are valuable in assessing ISC of organizations, majority frameworks are for large organizations and not for SMEs. For instance, [2], [20] presents assessment frameworks and methodology that aims at pinpointing what areas in information security need attention for ISC to thrive in an organization. The frameworks emphasize an assessment based on the availability of a well-defined information security policy and the availability of information security officers in the organization. Besides, the frameworks are suitable for assessing a single organization, which has a well-defined ISC in place. Since in most cases SMEs lack formalized ISC [3] applying these assessment frameworks for SMEs may be impractical.

Additionally, although framework by [3] was developed for SMEs, it lacks some of the factors that are necessary for SMEs in the SSA. Information security culture exists in its parent culture [18], and the SSA region's culture is different from that of Australia [17]. There is a need for assessment dimensions specific for SMEs in the SSA context, and method that can comprehensively assess ISC. Hence, organizational, and environmental dimensions consisting of factors for measuring ISC of SMEs in the SSA context are presented in Table 1.

Furthermore, most studies use a single assessment method. Assessment of ISC is complex, and it inherits its complication from the assessment of culture. One measurement method such as quantitative [2], [20] or qualitative [3] assessment is not enough to understand information security culture. Researchers propose that to understand the culture of an organization a combination of quantitative and qualitative tech-

niques must be utilized [16],[25]. It is proposed to conduct interviews with key personnel, observations, and questionnaires with the member of the groups. The succeeding section will explain the assessment method followed in detail.

Table 1. Information security culture assessment dimensions

	Sub-dimension	**Description**
Organizational Dimension	Top management support	Support for ISC from the SME's management (owners) through enterprise's vision and strategy necessary for the protection of the information resources. Allocation of resources for ISC issues as well as the trust between management and employees [21].
	ISP	Availability of formal or informal information security policy and procedures (ISP) that prescribes and states what is expected of employee's' behaviors for preserving information security of the SME [21]–[23].
	Risk assessment and management	Capabilities that an SME has in identifying, measuring, controlling and minimizing losses associated with security threats [2].
	SETA programs	Availability of resources to support SETA programs. Security training creates awareness of information security protections, technologies, requirements, risks, and threats [23], [24].
	Technical resources	Availability of security countermeasures, i.e., technical resources necessary for the protection of information systems, such as anti-malware, and firewalls [15].
	Human resources	Availability of either a part-time/full-time employee hired by the SME who qualifies to be an IT security expert such as an information security officer (ISO) [20], [25].
Environmental Dimension	National ISC initiatives:	Availability of government support on the promotion of national information security culture. Availability of strategic plans and guidance on information security culture to SMEs. Also, the availability of clear regulations on the protection of information and information systems resources [3], [26].
	International security standards:	The use of international standards such as COBIT or BS7799 that affects or influences the information security culture of an SME [27]–[29].
	IT suppliers/ vendors:	These are security technology suppliers or vendor that might persuade an SME to invest in security technology mostly it is for the vendor's benefit, but also affects the ISC consciousness of an SME [3].
	Partners organizations:	These can be any external organization that partners with an SME for business or as a supporting system. The partner organization might have their security policy that forces an SME to practice security conscious culture while communicating or doing business transactions with that partner.

3 Research methodology

Considering the challenging nature of the assessment of ISC as a whole, a combination of measuring items and data collection methods are recommended [8]. Hence to assess the organizational and environmental dimensions of the ISC of SMEs a combi-

nation of quantitative (survey) and qualitative (roundtable discussions and focus groups) methods were employed.

3.1 Instrument development

To improve the validity and reliability of results, we synthesized instruments from a comprehensive review of validated and tested survey instruments in the literature. The organizational dimensions included management support questions from Knapp et al. [21] information security policy and procedures from [21], [23], methods for risk assessment and management [20], SETA [23], technical and human resources. For the qualitative data, open-ended questions were used to complement the survey data. The qualitative data was essential to gain a more in-depth understanding of the status of the ISC of SMEs in Tanzania.

The survey instruments had two sections: the first section captured the enterprise data, which collected SMEs specific information such as the type of industry, number of employees and organization operation years. The second section captured the primary research data, this covered organizational and environmental dimensions. All primary research items were of five-point scale response format, the value of five (5) "strongly agree" and one (1) "strongly disagree" to show a respondent's level of agreement with the statements. Example survey questions: "*Our organization management takes security issues into account when planning organization strategies*"; "*Our government demonstrates strong commitment to encouraging information security culture*."

Pre-test of the survey instrument was done in two phases; the first phase included three doctoral students who reviewed the resulting survey instruments to identify unclear phrasing and determine the survey response time. Questions that seemed difficult to understand for an SME were removed or re-structure. The second phase included five volunteers, two representatives from the Tanzanian chamber of commerce industry and agriculture (TCCIA) and three SMEs. Final modifications were made to the instruments for distribution.

1.1 Case study organizations

In Tanzania, SMEs are considered a pillar of the Tanzanian economy contributing around 27% of the GDP [31]. Overall, SMEs account for about 3 million Tanzanian enterprises and employ approximately 93.3% of all Tanzanian workers [31]. SMEs categorization is based on turnover, numbers of employees and capital investment. Notably, those engaging one to 100 people with the capital investment of a maximum of 800 million Tanzanian Shillings (TZS) (1 USD = 2285 TZS). Tanzania's SME national policy refers to SMEs as micro, small and medium enterprises [30]. The micro-enterprises fall under the informal sector with a capital investment up to TZS 5 million and recruits up to four employees. Small enterprises are formalized employing between 5 and 49 staff and medium enterprises employ between 50 and 99 staff. These SMEs include a wide range of ventures that cover non-farm economic activities

manufacturing, mining, commerce, and services. The SMEs differs in their focus, technology innovations, and risk-taking attitudes.

3.2 Data collection

Data was collected from the SMEs situated in the city of Dar es Salaam, a prominent commercial capital of Tanzania located on the coast of the Indian Ocean. According to the Tanzanian SME Development Policy [30] and the national baseline survey on SME [31], the majority of SMEs are situated in Dar es Salaam. Recruitment of the subjects of this study was done through the Tanzanian chamber of commerce industry and agriculture (TCCIA)[1]. TCCIA has chambers in 21 regions, and 90 district centers; with the central office in Dar es Salaam. TCCIA is a private sector association established in 1988 with support from the Tanzanian government to strengthen and promote the development of privately owned enterprises. TCCIA receive backing from international organizations and government to promote training and mobilization of the business community. All respondents in this study were obtained from the TCCIA SMEs members' database.

Roundtable and focus group discussions. We organized one roundtable discussion in Dar es Salaam, Tanzania. Thirty-nine distinct SMEs took part in the study; representatives included SMEs owners, managers, and employees. This interactive setup of qualitative data collection is suitable for explorative studies that involve managerial people with a diverse organizational culture like SMEs. In addition, roundtable discussion stimulates the exchange of ideas and allows complex issues and factors to be discussed adequately. Apart from not only collecting data we also intended to create awareness of the need for ISC in the SME environment.

The roundtable discussion lasted 4 hours; the meeting was divided into five small discussion focus groups where each group consisted of 6 to 10 participants. Informed consent was reviewed and obtained in writing before starting discussions. Participants completed a demographic questionnaire and the main survey questionnaire before beginning discussions. Data were collected in the form of digitally audio-recorded sessions. Data were transcribed verbatim and analyzed thematically with Atlas.Ti. Data collected from the focus group discussions is used to complement the survey data in this paper.

Survey. Two survey modes, paper-based and web-based questionnaires were administered to the SMEs. The mixed-mode survey has been shown to be better in increasing the response rate from SMEs [32]. The paper-based questionnaires were distributed to 39 SMEs attendees of the roundtable discussion linked to this study, among those 26 responded to the survey. The online-based survey was distributed through TCCIA SMEs members e-mail list. One hundred and thirteen e-mails were sent, only fourteen SMEs responded to the survey.

The paper-based response rate was 68%, while online survey response rate was 12.4%. The online survey response rate was very low; nonetheless, studies [32, 33]

[1] http://www.tccia.com/tccia/

have shown that web-based survey has a lower response rate compared to the paper-based survey. Furthermore, research [33] indicate that lower electronic-based response rate is to be expected especially when the respondents include top managers than the employees, which was the case in our study. In total forty responses were received from the SMEs. Data was analyzed with SPSS Statistics software package. Screening of data for outliers, missing responses, non-normal distribution [34] and erroneous data was done to the data. Six incomplete responses were removed and resulted in 34 SMEs responses for analysis.

4 Analysis and discussion

This study presents 34 cases of SMEs from Tanzania; the majorities 18 of SMEs were small enterprises and 16 medium enterprises. Eighteen (18) of the respondents were SMEs owners, eight managers, and eight employees. Most SMEs (14) have been operating for 6-10 years, 10 SMEs operating for 11-20 years, 6 SMEs operating for more than 20 years and 5 SMEs operating from 3-5 years and 2 SMEs operating for less than three years. A wide range of SMEs industries was from agricultural services, finance banking, and insurance and Information and communication technologies. Fifteen (15) industries were represented with top being from Agriculture Services (7), Finance, banking and insurance (6), Information & communication technology (ICT) and Telecommunication (5), Retail & Wholesale merchandising(5), Manufacturing (3), Consulting services (3), Healthcare (3), Education (3), Legal (3), Tourism & Hotel (2), Transportation (2), Food Processing (2), Export (2), Oil & Gas (1) and Entertainment (1).

The next segments analyze the organizational and environmental dimensions to determine the status of ISC of SMEs in Tanzania. Due to the small sample size (n=34) data analysis is limited to descriptive analysis. The descriptive analysis included the means for measuring the central tendency and standard deviation (SD) for the average amount that a response deviated from the mean.

The overall mean is the interpretation of the mean values for a specific sub-dimension holding several statements. The responses were collected from a five-point Likert scale response format, for all items, the value of five (5 strongly agree) is the highest score, and one (1 strongly disagree) is the lowest score. Therefore, the mean score of 4.0 (agree) on a sub-dimension is used for indication of an acceptable level of information security culture. This cutoff point is similar to a 4.0 mean presented in the ISC assessment by Da Veiga & Martin [20]. Their study used a survey approach to assess the ISC of an organization by identifying what components of an organization was to be enhanced or obstructed to improve the protection of the organization's information.

4.1 Organizational dimension

The mean score values of organizational factors (Table 2) as computed from responses of 34 SMEs show no sub-dimension with an overall mean of 4.0 or higher.

Mean comparisons between small vs. medium enterprises were also computed as seen in Table 2. Results indicated a higher mean score for medium enterprises than small enterprises for all sub-dimensions.

Table 1. Organizational dimension means for SMEs in Tanzania

Organizational dimension	**Small Enterprises**		**Medium Enterprises**		**Overall**	
	Mean	**SD**	**Mean**	**SD**	**Mean**	**SD**
Technical resources	3.56	0.82	3.81	0.92	3.68	0.88
Top management support	3.37	0.99	3.67	0.71	3.5	0.87
SETA programs	2.94	0.90	3.33	0.66	3.12	0.81
ISP	2.97	0.99	3.27	0.81	3.11	0.91
Human resources	2.76	0.76	3.32	0.60	3.03	0.73
Risk assessment and management	2.81	1.06	3.28	0.73	3.03	0.94

Technical resources. Majority of SMEs appears to invest more in security technology than any other sub-dimensions. A higher technical resource mean score indicates that SMEs see technology tools as the key to their security problems. This result is in line to other SSA studies that report SMEs to be more interested in security technology [35]. Interestingly, qualitative findings support this observation. Majority of focus group participants expressed that their first thinking on security protection is to install anti-malware and firewall and consider their enterprises are safe with these technologies. In addition, participants from sectors such as agriculture services, finance, ICT, and telecommunication reported to use and prefer cloud computing for their business. These SMEs believed that their data are safe in the cloud. "*Yes, of course, we have normal measures, for instance, all our documents are saved in the cloud. If a person quits, they can no longer access our organizational document because once we remove the person from the cloud, they can no longer access our information. Also, it is easy to track the projects trail, who saved and who deleted from the cloud, we have a lot of restrictions in place [SME_R3a]"*

... the good thing is it is sitting somewhere in the cloud, so it does not matter, even if the person loses the laptop. [SME_R2a]

Top management support. Top management support is the most significant factor in influencing the cultivation of ISC in the organization [21]. However, in this study, the results showed an incredibly low mean value of 3.5 compared to the technology investment. This poor top management support for ISC reflected on the investment of other sub-dimensions such as information security policy, the absence of SETA programs, lack of human resource investment and inadequate risk assessment and management.

The findings from the focus group indicated a lack of facts about ISC as the main obstacles in top management support of ISC. SMEs owners and managers are aware of information security but lack the know-how on the cultivation of ISC and the importance of strategizing about ISC to their organizations. The size of the enterprises influenced how SMEs saw the importance of ISC in their organization. Participants reported their size and lack of financial resources as the hindrance factors. "*You know how to handle information security differs. For example, for my business, I do not know the importance of information security. Those who are in the large organization they might know because they have a lot to lose. For SMEs like us, it is hard to deal with security; it is expensive*."

ISP. Results from the focus group showed a strong perception that the size of the organization determined the formality of SME's information security policy and procedure. Verbal ISP reminders seemed to be the approach preferred by most SMEs . *"Our information policy is implemented verbally; people know what not to do. Moreover, we have antivirus and firewall our policy is implemented there" [SME_R1a].*

Risk assessment and management. In this construct, 67.6% (n=23) of SMEs reported that risk assessment was too complex for their organizations. Participants reported a lack of measures for assessing and managing security incidents and a lack of pre-predefined procedures in case of security incidents. Moreover, majority of the participants reported that their organizations conduct fewer or no assessments of their systems.

Human resources. SMEs management biggest concern was the complexity of hiring a full time IS security expert due to lack of finances and lack of trust.... *Let us say we are using one system. I do not want to hire an IT specialist because, one, it is not cost effective. And another thing, I think I am not utilizing him fully. Even if I employ the person, on the salary that I am paying he is [probably] working for one or two hours for the rest of the day. [This way] I am not utilizing the person properly. This is what we always feel as employers. Ooh, now if I outsource, [I think about] my information, someone else can look at it and hack. So that is something that comes up, that we do not outsource…, we also don't want to employ an IT personnel. So that is where the problem arises[SME_R2a].*

1.2 Environmental dimension

Like the organizational dimension, the environmental dimension (Table 3) results indicated a higher mean score for medium enterprises than small enterprises. The mean values of the variables ranged from 2.85 to 3.49. SMEs responses show that their ISC is more influenced by vendors (3.38) and partner organization (3.49) than the national ISC initiatives (2.91). Overall, the environmental factors in Table 3 show that SMEs are unsure of the existence of environmental support for the ISC of SMEs in Tanzania.

Table 1. Environmental dimension means for SMEs in Tanzania

Environmental dimension	Small Enterprises	Medium Enterprises	Overall

	Mean	SD	Mean	SD	Mean	SD
Partner organization	3.38	0.22	3.61	0.25	3.49	0.97
Vendor pressure	3.11	0.29	3.66	0.24	3.38	1.13
National ISC initiatives	2.72	0.16	3.11	0.15	2.91	0.68
International security standards	2.33	0.26	3.37	0.19	2.85	1.06

Partner organization and vendor pressure. From the environmental dimension, we see that SMEs' partner organizations and vendors mean score were higher than the rest of the sub-dimensions. This shows that SMEs are more likely to be persuaded to invest in security technologies by vendors and their business partners. IT vendor and partners influence were reflected in SME's choice of cloud computing, many report cloud computing as the best and secure way to store data. "*…cloud computing is the thing. We host remotely; we choose the partners who are serious with IT security [SME_R4a].*" However, literature shows that cloud computing does not always guarantee security [37] because the security of data in the cloud is to a higher extent user's (subscriber's) responsibility and not only service provider's.

National information security culture initiatives. There was a consensus among participants of the focus group that in Tanzania there are poor national initiatives for the cultivation of ISC in SMEs environment. "*Lack of information security culture in our organizations is not about the country's national culture, but it is [just] lack of information security culture in the country*" [SME_R1a].

Most SMEs were unaware of the national information security related laws, regulations, national acceptable standards, or even international security standards. Tanzania for instance is a member of the International Organization for Standardization (ISO) through Tanzania Bureau of Standards (TBS). However majority of SMEs are unware of recommended information security strategies or framework to follow. When reporting on the influence of international security standards, only two SMEs (medium enterprises) dealing with information and communication technology business indicated to be aware of and use international information security standards such as ISO 27001.

Scholars argue that national initiatives for ISC can be a positive contributor to motivating SMEs to engage in security protection actions [3]. As it has been for IT adoption [36], external support, such as government and private sectors initiatives can directly stimulate information security practices of SMEs. In Tanzania, SMEs are expected to receive institutional support from different government and parastatal organizations. The Tanzania SME policy [30], mentions information technology-based institutions such as the Tanzania Commission for Science and Technology (COSTECH) and Tanzania Communications Regulatory Authority (TCRA). However, SMEs reports a lack of institutional support especially on issues related to Information security culture. SMEs in Tanzania requires external support such as gov-

ernment institution to push for the cultivation of ISC in SMEs environment as it is done in other countries [26].

5 Conclusion

The findings of this exploratory study show an unfavorable status of the ISC of the participating SMEs in Tanzania. The results and implications of these findings suggest further research and intervention is necessary to institutionalize ISC in the SME environment. This study proposes the development of frameworks for the institutionalization of ISC of the SME in SSA environment using design science research. We also call for the national level ISC initiatives to motivate SMEs to nurture ISC. Furthermore, there is a need for theoretical based national level SETA-programs interventions to SMEs owners, managers, and employees. The main limitation of this study was the small sample size on a quantitative part of the study; future research may benefit from a larger sample size by including SMEs from other regions of SSA for a cross-country comparison to identify country-specific factors.

6 Bibliography

1. Verizon Business, "2018 Data breach investigations report," *Trends*, pp. 1–62, 2018.
2. Da Veiga A. and Eloff JH., "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2010.
3. Dojkovski S., Lichtenstein S., and Warren M., "Institutionalising information security culture in Australian SMEs : Framework and key issues," in *International Symposium on Human Aspects of Information Security & Assurance*, 2007, pp. 10–24.
4. Tolah A., Furnell SM., and Papadaki M., "A Comprehensive Framework for Cultivating and Assessing Information Security Culture," in *The Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 2017, pp. 52–64.
5. Van Niekerk J. and Von Solms R., "Understanding Information Security Culture: A Conceptual Framework," *Proc. ISSA 2006*, May, pp. 1–10, 2006.
6. Alnatheer M.and Nelson K., "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.," *7th Aust. Inf. Secur. Manag. Conf.*, 2009.
7. Thong J.Y.L. and Yap C.S., "Information technology adoption by small business: An empirical study," pp. 160–175, 1996.
8. Schlienger T. and Teufel S., "Information security culture – from analysis to change," *South African Comput. J.*, vol. 31, pp. 46–52, 2003.
9. Ponemon Institute LLC, "2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB) Sponsored by Keeper Security," 2017.
10. Straub D., Loch K., Evaristo R., Karahanna E., and Srite M., "Toward a Theory-Based Measurement of Culture," *J. Glob. Inf. Manag.*, vol. 10, no. 1, pp. 13–23, 2002.
11. Karjalainen M., Siponen M. T., Petri P., and Suprateek S., "One size does not fit all: Different cultures require different information systems security interventions," in *IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, 2013.
12. Whitman M. E. and Mattord H. J., "Principles of Information Security. Fourth Edition," *Course Technol.*, p. 617, 2012.

13. Mitnick K. D.and Simon W. L., *The art of deception: Controlling the human element of security*. WIley Publishing, 2011.
14. Herath T. and Rao H. R., "Encouraging information security behaviors in organizations : Role of penalties , pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.
15. Thomson K.-L., Von Solms R., and Louw L., "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, 2006.
16. Schein E. H., "Coming to a New Awareness of Organizational Culture," *Sloan Manage. Rev.*, vol. 2, pp. 3–16, 1984.
17. Hofstede G., "Cultural dimensions in management and planning," *Asia Pacific J. Manag.*, vol. 1, no. 2, pp. 81–99, 1984.
18. Schein E. H., *Organizational Culture and Leadership*, 3rd ed. Jossey-Bass, 2004.
19. Alhogail A., "Information Security Culture : A Definition and A Literature Review," *IEEE*, 2014.
20. Martins N. and Da Veiga A., "Information Security Culture : A Comparative Analysis of Four Assessments," *Eur. Conf. Inf. Manag. Eval.*, no. September, pp. 49–58, 2014.
21. Knapp K. J., Marshall T. E., Kelly Rainer R., Nelson Ford F., Rainer R. K., and Ford F. N., "Information security: management's effect on culture and policy," *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006.
22. Kinnunen H. and Siponen M., "Developing Organization-Specific Information Security Policies," in *PACIS 2018*, 2018, pp. 1–13.
23. Chen Y. A. N., Ramamurthy K. R. A. M., and Wen K., "Impacts of comprehensive information security programs on information security culture," *J. Comput. Inf. Syst.*, vol. 55, no. 3, p. 11, 2015.
24. Siponen M. T., "Five Dimensions of Information Security Awareness," *Comput. Soc.*, no. June, pp. 24–29, 2001.
25. Schlienger T. and Teufel S., "Analyzing information security culture: Increased trust by an appropriate information security culture," *Proc. - Int. Work. Database Expert Syst. Appl. DEXA*, vol. 2003–Janua, pp. 405–409, 2003.
26. Enisa, "Information security and privacy standards for SMEs," *European Union Agency For Network And Information Security*, no. December. 2015.
27. Sipior J. C. and Ward B. T., "A Framework for Information Security Management Based on Guiding Standards : A United States Perspective," *Issues Informing Sci. Inf. Technol.*, vol. 5, pp. 51–60, 2008.
28. Von Solms B., "Information Security — The Third Wave ?," *Comput. Secur.*, vol. 19, pp. 615–620, 2000.
29. Siponen M. and Opinion T., "Information security standards focus on the existence of process, not its content," *Commun. ACM*, vol. 49, no. 8, p. 97, 2006.
30. URT, "Small and Medium Enterprise Development Policy," *J. SMEs policies*, vol. II, no. April, pp. 12–20, 2003.
31. Ministry of Industry and Trade, "National Baseline Survey Report for Micro, Small and Medium Enterprises in Tanzania," *Ministry of Trade and Financial Sector Deepening Trust*, vol. 53, no. 9. 2012.
32. Meckel M., Walters D., and Baugh P., "Mixed-mode surveys using mail and web questionnaires," *Electron. J. Bus. Res. Methods*, vol. 3, no. 1, pp. 69–80, 2005.
33. Fan W. and Yan Z., "Factors affecting response rates of the web survey: A systematic review," *Comput. Human Behav.*, vol. 26, no. 2, pp. 132–139, 2010.
34. Heiman G. W., *Basic statistics for the behavioral sciences*. Cengage Learning, 2013.

35. Bougaardt G. and Kyobe M., “Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa,” *Electron. J. Inf. Syst. Eval.*, vol. 14, no. 2, pp. 167–178, 2011.
36. Ghobakhloo M., Hong T. S., Sabouri M. S., and Zulkifli N., “Strategies for successful information technology adoption in small and medium-sized enterprises,” *Information*, vol. 3, no. 1, pp. 36–67, 2012.
37. Chen D. and Zhao H., “Data Security and Privacy Protection Issues in Cloud Computing,” *2012 Int. Conf. Comput. Sci. Electron. Eng.*, no. March 2012, pp. 647–651, 2012.