Assessing Information Security Culture: A Critical Analysis of Current Approaches

Irene Okere
The school of ICT
Nelson Mandela Metropolitan University (NMMU)
Port Elizabeth, 6031
South Africa
Email: Irene.Okere2@nmmu.ac.za

Johan van Niekerk
The school of ICT
Nelson Mandela Metropolitan University (NNMU)
Port Elizabeth, 6031
South Africa
Email: Johan.vanniekerk@nmmu.ac.za

Mariana Carroll
Deloitte & Touche
Risk Advisory
Woodlands, Docex 10
South Africa
Email: mcarroll@deloitte.co.za

Abstract— Today's businesses operate in an interconnected and global environment allowing them to collaborate with one another and share information resources. At the same time this interconnectivity exposes the organization to many internal (employees) and external threats. Internal threat is among the top information security issues facing organizations as the human factor is regarded the weakest link in the security chain. To address this "human factor" researchers have suggested the fostering of an information security culture to address the human behavior so that information security becomes a second nature to employees. An important step in the fostering of an information security culture is the assessment of the current state of the culture. This paper focuses on the analysis and comparison of current information security culture assessment approaches, to evaluate their suitability specific for use in the culture change process.

Keywords- Information security culture, assessment, culture change

I. INTRODUCTION

Today's organizations operate in a global environment. Globalization enables organizations to collaborate and share information resources with one another but also exposes them to many threats both within and from outside of the organization. Organizations therefore need to secure their information resources.

Humans are largely at the center of protecting an organization's information resources through their behavior when interacting with information and information systems. Through the formulation of information security policies, management requires employees to behave in a secure manner and consequently protect information resources. However, employees are known not to adhere to the security policies, leading to security breaches [1,2].

To mitigate the risk posed by the non-adherence of employees to security policies (the "human factor"), researchers suggest the fostering or development of a culture of information security (information security culture) [3-5].

The first step in the development of an information security culture is the assessment of the current state of the culture [6]. According to Schlienger & Teufel [7,8], there is no unique toolset and method for studying information security culture with regards to what to assess and how to assess information security culture. The problem therefore exists that there is no published widely accepted and consolidated approach that indicates how the assessment of information security culture should be done and researchers have called for more research in this area [7-9].

This paper focuses on the analysis and comparison of current approaches to the assessment of information security culture in order to ascertain their suitability specific for use in the culture change process. The remainder of this paper will briefly describe the methodology used (section II); introduce the concept of an information security culture (section III); examine the process for fostering such a culture and discuss the role culture assessment plays in the fostering and management of an information security culture (section IV); critically evaluate and compare current approaches to the assessment of an information security culture (Section V); and finally discuss the outcome of section V (section VI). Section VII concludes this paper by proposing the use of an audit framework for the assessment of information security culture.

II. METHODOLOGY

This research performs a critical analysis on current (existing) information security culture assessment approaches through a combination of literature reviews and qualitative content analysis techniques.

Qualitative content analysis is a "research method for the subjective interpretation of content of text data through the systematic classification process of coding and identifying themes or patterns" [10]. The analysis was conducted according to guidelines provided by Krippendorff [11]. A literature study was conducted and a number of research projects that focus on the assessment of information security culture were identified. The main idea of each article under review was identified and the article's strengths and weaknesses were analyzed. Qualitative content analysis was done on the identified research based on the following broad thematic areas:

- Did the researchers assess the following levels of information security culture: artifacts, espoused values, shared tacit assumptions and information security knowledge?
- What assessment methods were used to assess which level of information security culture?
- Did the researchers use an integrated approach incorporating all levels of information security culture?

The results from the critical analysis, based on these three thematic areas are discussed in section V and VI as the outcome of this paper.

III. Information Security Culture

Security does not lie only in firewalls, passwords and awareness training but also in a culture that views and thinks correctly about information security issues. A culture of information security needs to be embedded into the organizational culture, to allow them to view and think correctly about information security problems [12].

Information security culture is a subculture of organizational culture [7]. It is mostly described using Schein's model of organizational culture which is widely accepted in the field of information security [7, 8]. According to Schein [14] organizational culture is "a pattern of shared tacit assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". Schein describes culture as existing in three levels: artifacts, espoused values and shared tacit assumptions. This definition however is not specific to information security despite being widely accepted as a general organizational culture definition hence the enhancement by Van Niekerk & Von Solms [15].

Van Niekerk & Von Solms [15] describes information security culture by adapting Schein's model and adding a fourth level, information security knowledge which supports the other three levels. Information security knowledge is necessary if employees are to behave in a secure manner, as it cannot be assumed that the employees possess such security knowledge. The four levels of information security culture are described below.

- *Artifacts:* This is the visible layer, referred to as the surface manifestation of culture [13]. Artifacts are the things that are observed in an organization [14] and refer to visible and measurable everyday behavior in the organization [3]. Artifacts include behavior patterns, security handbooks, awareness courses, language and technology. This level though visible is hard to interpret without questioning the "insiders" of the organization.
- *Espoused values:* This layer is partially visible and unspoken but can shape the behavior of employees [13]. Espoused values represent the "reasons" given by insiders of an organization regarding the observed artifacts [14]. The espoused values of an organization include strategies, goals, philosophies and other documents that describe the values, principles and vision of the organization [14].
- *Shared tacit assumptions:* Shared tacit assumptions usually form in organizations that have been successful where the success can be attributed to the values, beliefs and assumptions of the founders of the organization [14]. If the organization continues to be successful, the beliefs and values become shared and taken for granted and form the core of the organization's culture [16].
- *Information security knowledge:* This level supports the other three levels: 1) *artifacts* (employees need to have adequate information security knowledge of how to carry out their job functions in a secure manner), 2) *espoused values* (the relevant employees need to have sufficient information security knowledge to know what to incorporate into a policy document for example, to ensure that it adequately addresses the security needs of the organization), and 3) *shared tacit assumptions* (if an employee's beliefs conflicts with an espoused value for example, not knowing why a specific control is required, the employee might knowingly disregard the security control). Knowledge could thus help in ensuring compliance [8].

IV. The Role Of Assessment In Culture Change

According to Cameron & Quinn [17] change is a given and organizations are subject to change in order to survive. Change in an organization needs to be properly managed to avoid failure. This failure can sometimes be attributed to the neglect of organizational culture. Organizations therefore need to manage the change process at the cultural level [17].

Schein [16] proposes a structured change management process to facilitate culture change in the organization. Successful culture change needs to start with support from top management [18]. Fig. 1 illustrates a culture change process adapted from Van Niekerk & Von Solms [3] and is described below.

- *Step 1: Top management support and commitment*

  Management needs to understand the existing culture (current state), the need for change and the idea of change usually in response to a "business problem".

- *Step 2: Define the specific business problem*

  This entails assessing the current state of culture, defining the preferred future state of culture and analyzing the gap between the current and the preferred state. The steps needed to move from the current state to the preferred state follows a transformative change management process [16]. According to Schein [14] such a transformative process involves three stages: 1) unfreezing (creating motivation for change through disconfirmation and psychological safety), 2) learning new concepts and new meanings for old concepts through imitation of and identification with role models, 3) refreezing (internalizing the new concepts and new meanings). O'Donovan [18] suggests using "culture embedding mechanisms" like modeling, teaching and coaching by leaders to internalize the new way of doing things into everyday practices.

- Step 3: Develop strategic action plan

  Strategic action plans include: Identifying actions and behaviors that need to be started, stopped or encouraged towards achieving the kind of behavior that aligns with the desired culture; evaluating employees' readiness for change; educating the employees regarding the culture change to minimize resistance; motivating the employees; generating social support by involving those affected by the change and identifying champions who can influence others and act as role models; providing constant and extensive information to increase employees' understanding and commitment to minimize confusion and resistance and to prepare them for the effects of the change.

- Step 4: Create a cultural fit

  Creating a cultural fit through mechanisms like education and training, appraisal and reward systems helps to ensure that the changes last. O'Donovan [18] refers to such mechanisms as "embedding mechanisms".

- Step 5: Develop and choose a change leader team

  This is necessary to facilitate the change. The leaders need to be committed, competent and have a common purpose.

- Step 6: Create small wins

  It is important to identify key action steps that can be executed to generate momentum. Such small actions must be aligned to the desired culture change for motivation of employees.

- Step 7: Identify metrics, measures and milestones

  It is important to identify measures for success, metrics of the main indicators and milestones to track progress of the change. As the change process progresses it may be necessary to *reassess* the current state following the results emanating from tracking the change process.

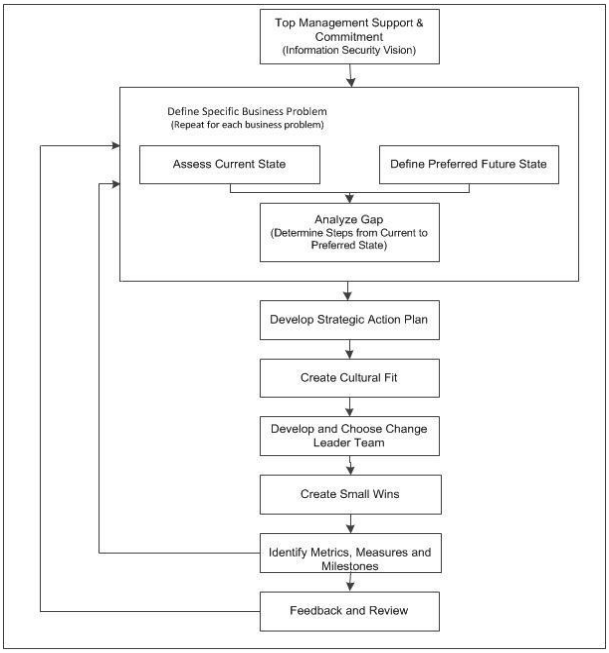

Fig. 1 Framework for culture change adapted from Van Niekerk & Von Solms [3]

- Step 8: Feedback and review

  The organizational environment changes frequently due to internal and external factors and so does the organization's needs. It therefore becomes necessary to periodically review and refine the entire information security culture management process. The feedback and review can necessitate the *reassessment* of the current state of information security culture in order to ensure that the organization's information security culture is continuously managed and the organization's security needs are met.

Assessment plays an important role in the culture change process, as illustrated in the eight-step culture change process. Culture is a complex, extensive and multifaceted concept that needs to be analyzed and assessed at each level in order for it to be understood [14]. The complexity of culture is implicated in the mission, vision, strategy and goals of the organization (external survival issues), and in the relationships amongst people in the organization (internal integration issues). These are also correlated to the broader national cultural assumptions arising from organizations becoming global.

Culture assessment could be used to solve a business problem, make something more efficient, or to achieve a new strategic goal possibly arising from mergers, joint ventures or partnerships incorporating more than one culture [14]. According to Schein [14] assessment of culture plays an important role in culture change. It helps an organization to understand its own culture in terms of strengths and weaknesses and assist to make strategic choices. Consequently, culture assessment enables an organization to solve a problem, to make a change and to learn something new. In order to do

this, an organization needs to know how the culture or subculture can help or deter it.

According to O'Donovan [18], culture change exists in response to internal and external forces in the environment. Internal forces include technology, policies, leadership changes, absenteeism, and rapid staff turnover while external forces include political, economic, environmental and regulatory forces. These forces can necessitate the assessment of culture. For example, a new chief executive officer/chief security officer has a new security vision that could necessitate assessment of the information security culture to align with the new security vision. As explained, one of the reasons for culture assessment is to solve a "business problem". One such problem could be information security that necessitates culture assessment in order to identify improvements to the security policy. Culture assessment could also arise due to organizations having to comply with regulatory and/or legal requirements and/or standards, for example the health insurance portability and accountability act of 1996 (HIPAA) which deals with the protection of personal healthcare information either stored or in transit within or outside of the organization [12], the Sarbanes-Oxley act of 2002 which requires organizations to independently certify the adequacy of their internal controls [19], and the ISO 27001 which stipulates the requirements for implementing security controls to meet the needs of every organization [20].

According to Martins & Eloff [21] assessment in culture change can also help to ensure that recommendations from previous assessments are implemented. Conducting periodic assessments, implementing solutions and addressing the concerns arising from previous assessments can constantly improve the organization's information security culture. Culture assessments also assist an organization to identify the current and the desired information security culture, the areas that need the most attention, and improvements needed to achieve the desired information security culture [22]. Another reason for culture assessment is to help an organization understand the behavior of its employees towards information security and to identify key issues for implementation and integration into the information security culture of the organization [23]. Assessment of information security culture can also serve as a "wake-up" call for management depending on the results of the assessment and to take decisive action [6].

Having highlighted the importance of assessment in culture change, it is necessary to discuss approaches that can be used towards the assessment of information security culture.

V. CURRENT ASSESSMENT APPROACHES

From the literature analysis conducted, a number of research projects were identified that focus on the assessment of information security culture in an organization, namely Maynard, Ruighaver & Chia; Martins & Eloff; Ngo, Zhou, Chonka & Singh; Gerbrasilase & Lessa; Schlienger & Teufel; Finch, Furnell and Dowland; [9,21-25].

Martins and Eloff used an assessment approach consisting of an audit process and including an information security culture questionnaire for the assessment of information security culture in an organization. Ngo, Zhou, Chonka & Singh discussed how the level of information security culture in Australian small and medium enterprises can be assessed. Gerbrasilase & Lessa used a descriptive survey method for the assessment of information security culture in Hawassa referral hospital. Schlienger & Teufel used an information security culture management process incorporating a combination of methods for the assessment and management of information security culture in an organization. Finch, Furnell & Dowland assessed the information security culture by targeting the security attitudes and perceptions of system administrators and end-users to ascertain any disparity between both perspectives. Maynard, Ruighaver & Chia developed a research model for information security culture which can be used to assess the quality of an organization's information security culture.

This paper focuses only on the two assessment approaches that describe a process for the assessment of information security culture in an organization namely Martins & Eloff, Schlienger & Teufel [21,24]. Both assessment approaches will be discussed in this section to determine their suitability specific for use in the culture change process.

A. *Martins and Eloff's assessment approach*

Martins & Eloff [26] argue that employees' behavior and their interaction with computer systems play a major role in the security of information. They argue that employees need to display an acceptable behavior with regards to information security which should translate to their everyday activity in the organization.

The researchers suggest that organizational behavior needs to be considered in the development of the desired organizational culture. They propose incorporating organizational behavior theory in order to instill information security culture. This was done through the development of an information security culture model consisting of three levels: organization, group and individual. They identified certain issues at each level that could promote information security culture and these issues (i.e. policy and procedures, risk analysis at the organization level, management and trust at the group level, awareness and ethical conduct at the individual level) are affected by change agents, namely technology or competition to achieve a certain information security culture.

To determine if information security culture is at an acceptable level in an organization, the researchers propose an assessment approach consisting of an audit process. The assessment approach aims to determine employees' perceptions, attitudes, opinions and actions towards information security. From the analysis of the information gathered throughout the audit, organizations can address information security culture issues at the three different levels (i.e. organization, group and individual). The audit process consists of four phases:

- *Phase 1*: Development of the assessment instrument (questionnaire). The assessment instrument was validated for reliability and validity [27].
- *Phase 2:* A survey process that utilizes the questionnaire from phase one to assess the organization's information security culture. The

researchers propose this assessment to be a continuous process in order to promote information security culture in an organization.

- *Phase 3:* Analysis of data obtained from phase two that gives a quantitative indication of the status of information security culture in the organization.
- *Phase 4:* Interpretations and recommendations concerning the analyzed data from phase three. This step provides feedback to the organization regarding their information security culture and to assist the organization in addressing areas of concern.

The following paragraphs outline Martins and Eloff's assessment approach with consideration to the three thematic areas outlined in section II.

1) *Did the researchers assess the following levels of information security culture – artifacts, espoused values, shared tacit assumptions and information security knowledge*?

- The researchers did not assess artifacts directly.
- The researchers did not assess espoused values directly.
- The researchers focused on perceptions, attitudes and behavior. It is therefore inferred that they assessed shared tacit assumptions.
- They assessed security knowledge but not comprehensively [27].

2) *What assessment methods were used to assess which level of information security culture?*

- No assessment method was used to assess artifacts directly.
- No assessment method was used to assess espoused values directly.
- A questionnaire was used to assess shared tacit assumptions.
- A questionnaire was used to assess security knowledge.

3) *Did the researchers use an integrated approach incorporating all levels of information security culture in their assessment?*

- The researchers used an auditing approach but did not incorporate all the levels of information security culture in their assessment.

B. *Schlienger and Teufel's assessment approach*

According to the researchers, information security culture needs to be maintained and modified continuously to ensure that it meets the organization's targets [8]. This continuous process of analysis and change referred to as the information security culture management process involves four stages: diagnosis, planning, implementation and evaluation:

- *Diagnosis:* This stage analyzes the existing information security culture and identifies any problems. There are two aspects to analyzing information security culture. The first is what to analyze (the assessment items) and the second is how to analyze (the assessment methods). The researchers propose a combination of assessment items and methods due to the difficulty in understanding culture.
- *Planning*: This stage involves two aspects. The first aspect is strategic planning which involves defining the target or objective for the development of information security culture of which the researchers used the information security policy and defining the market segments like employees, information technology staff and managers for comparison of data. The second aspect is operative planning which involves internal communication in terms of awareness programs, training, education and management buy-in in order to promote the security awareness of employees and managers.
- *Implementation:* This stage involves management commitment, communication with all employees, education and training for all employees, and employee commitment. During this stage, detailed activities, responsibilities, resources, schedules and a budget need to be defined [24].
- *Evaluation:* This stage gives information regarding the efficiency and effectiveness of the implemented actions.

The researchers used a combination of methods to assess information security culture. They started by analyzing the information security policy in order to understand the official values (espoused values) and the interpretation was validated by interviewing the chief security officer (CSO). Analysis of the security policy also formed part of the assessment of artifacts. The researchers developed a questionnaire to determine the perceptions and attitudes of employees (true values), the perceptions and attitudes of the organization (official values), and what the employee thinks should be the best solution for each question. Unstructured interviews were conducted with the CSO and a technician responsible for security. Firstly, the interviews were conducted before analyzing the security policy in order to get an insight of the organization's information security. Secondly, the interviews were conducted after analyzing the security policy in order to discuss and interpret the identified issues in preparation of the questionnaire. Interviews were also done after analyzing the results of the questionnaire in order to discuss the quality of answers given by respondents. Observation was done as part of assessing artifacts by comparing the respondent's answers with their behavior.

The following paragraphs outline Schlienger and Teufel's assessment approach with consideration to the three thematic areas outlined in section II.

1) Did the researchers assess the following levels of information security culture – artifacts, espoused values, shared tacit assumptions and information security knowledge?

- The researchers assessed artifacts, espoused values, shared tacit assumptions but did not assess security knowledge.

2) What assessment methods were used to assess which level of information security culture?

- The researchers used document analysis, interview and observation to assess artifacts.
- To assess espoused values the researchers used document analysis, questionnaire and interviews.
- They used a questionnaire to assess shared tacit assumptions.

3) Did the researchers use an integrated approach incorporating all levels of information security culture in their assessment?

- The researchers used an integrated approach but did not incorporate all four levels of information security culture in their assessment.

C. Summary of limitations of the two assessment approaches

According to Schein [14] culture should be assessed across all its levels. Neither of the assessment approaches assessed the four levels of information security culture as described in section III.

Both assessment approaches used a questionnaire to assess shared tacit assumptions. According to Schein [9, 25] a questionnaire or survey cannot be used to assess culture. This is because the dimensions of culture selected for assessment may not be important in relation to the cultural dynamics of that specific organization. Interviewing only the security personnel, as done by Schlienger & Teufel, may not reveal the problem the organization is trying to solve in its entirety. This will consequently affect what questions to ask and what questions to include in the questionnaire. In addition, the responses to the questionnaire cannot be evaluated to determine reliability and validity especially with the promise of anonymity and privacy, and because the respondents may understand and interpret the questions differently.

According to Schein [14] other issues with using a questionnaire to assess culture include:

- Questionnaires do not reveal the interaction and patterning in the cultures and subcultures.
- Only superficial characteristics of the culture will be assessed because survey instruments cannot get at the deeper shared tacit assumptions that define the essence of cultures.
- Due to the tacit nature of cultural assumptions, respondents of questionnaires will not be able to answer the survey questions reliably since there is no certainty as to how the respondents interpret the questions.
- Inferring shared assumptions from individual responses is very ineffective because individuals perceive questions differently.

Schlienger & Teufel interviewed the CSO to get an insight of the organization's information security but this will only provide a perspective of that of the CSO and not a true reflection of the entire organization's information security. Also by interviewing the security personnel after analyzing the questionnaire results does not give the interpretation for the respondents' answers but rather what the security personnel thinks the respondents mean.

Information security culture should be assessed across all its underlying levels, namely artifacts, espoused values, shared tacit assumptions and information security knowledge. Table 1 summarizes how the above researchers have assessed information security culture in an organization against the identified thematic areas, to determine if the different researchers assessed the four levels of information security culture, and the methods used in the assessment as well as the validity and reliability of the methods.

TABLE I. RESEARCH APPROACH, ASSESSMENT ITEMS AND METHODS

Assessment item	**Assessment method**	**Research approach**	
		Martins and Eloff	**Schlienger and Teufel**
Artifacts	Document analysis	None	Analysis of information security policy
	Interview	None	Interview **only** with CSO
	Observation	None	Audit with **no** formal auditing guidelines or procedure
Espoused values	Document analysis	None	Analysis of information security policy
	Questionnaire	No direct assessment	Questioning all level of employees
	Interview	None	Interview **only** with CSO
Shared tacit assumptions	Questionnaire	Questioning all level of employees	Questioning all level of employees
	Interview	None	Interview **only** with CSO
Information security knowledge	Questionnaire	**Few** knowledge questions	**No** direct assessment

VI. DISCUSSION

From section V it is evident that neither of the assessment approaches analyzed has an integrated approach for assessing all the underlying levels of information security culture as described in section III.

Schlienger & Teufel [7] focused on the assessment of artifacts, espoused values and shared tacit assumptions but not information security knowledge. Audit-based techniques were used only in the assessment of artifacts. However, no formal auditing guidelines or established auditing framework was used which makes it difficult for the exact same assessment to be replicated in another organization, or by other researchers.

Martins & Eloff focused mainly on shared tacit assumptions. Information security knowledge was not comprehensively assessed as acknowledged by the researchers [27]. Martins & Eloff [21] used an auditing approach in their assessment of information security culture but also did not explicitly state that formal auditing guidelines or framework was used.

It is also evident from section V that shared tacit assumptions have been addressed extensively by both assessment approaches. However, the assessment of artifacts, espoused values and information security knowledge is currently lacking. It is the assertion of this paper that formal auditing processes, as an integrated approach, can play a role in the assessment of the dimensions of information security culture. Part of the assessment of information security knowledge should also be to assess the level of employee knowledge. This can be included in security related educational programs in an organization. Assessment of information security knowledge should also form part of the audit process to ensure that employees are knowledgeable about information security. This is an important recommendation to ensure responsibility for security violations.

VII. CONCLUSION AND FUTURE WORK

This paper provided a critical analysis of the current approaches used in the assessment of information security culture. It is evident that the current approaches, though thorough in some aspects, do not present an integrated approach that comprehensively assesses all the levels of information security culture. The current approaches to the assessment of information security culture utilize some form of auditing either as an assessment method or approach. However, none have followed a formal auditing approach utilizing an established audit framework so that the assessment process can be replicated in another organization. The development of such an audit framework for the assessment of information security culture forms part of our future work in this area.

ACKNOWLEDGEMENT

The financial assistance of National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.

REFERENCES

[1] PWC, *Information Security Breaches Survey 2010 technical report*, 2010.

[2] Computer Security Institute, *14th Annual CSI Computer Crime*, 2009.

[3] J. Van Niekerk and R. Von Solms, "An holistic framework for the fostering of an Information security sub-culture in organizations.," *ISSA*, 2005.

[4] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information security culture," *Computer Fraud & Security*, vol. 2006, 2006, pp. 7 - 11.

[5] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, May. 2004, pp. 191-198.

[6] ISACA, "Creating a Culture of Security," *ISACA*, 2011.

[7] T. Schlienger and S. Teufel, "Analyzing Information Security Culture : Increased Trust by an Appropriate Information Security Culture," *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, 2003.

[8] T. Schlienger and S. Teufel, "Information security culture – from analysis to change," *Proceedings of ISSA*, 2003, pp. 183-195.

[9] S. Maynard, A. Ruighaver, and P. Chia, "Exploring Organisational Security Culture : Developing a comprehensive research model .," *IS ONE World Conference, USA*, 2002, pp. 1-13.

[10] H.-fang Hsieh and S. Shannon, "Qualitative Health Research," *Health (San Francisco)*, vol. 15, 2005, pp. 1277-1288.

[11] K. Krippendorff, *Conceptual foundation. In content analysis: An introduction to its methodology.*, Thousand oaks. CA. Sage, 2004.

[12] H. Tipton and M. Krause, *Information Security Management Handbook*, Auerbach Publications, 2007.

[13] A. Huczynski and D. Buchanan, *Organizational Behaviour: An Introductory Text*, FT Prentice Hall, 2007.

[14] E. Schein, *The Corporate Culture Survival Guide*, San Francisco: Jossey-Bass, 2009.

[15] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Computers & Security*, vol. 29, Jun. 2010, pp. 476-486.

[16] E. Schein, *The corporate culture survival guide*, Jossey-Bass, 1999.

[17] K. Cameron and R. Quinn, *Diagnosing and changing organizational culture: Based on the competing values framework*, Jossey-Bass, 2011.

[18] G. O'Donovan, *The corporate culture handbook: how to plan, implement and measure a successful culture change.*, the Liffey press, Ashbrook House, Ireland, 2006.

[19] H. Tipton and M. Krause, *Information Security Management Handbook*, Auerbach publications CRC Press LLC, 2008.

[20] ISO/IEC 27001, "Information technology — Security techniques — Information security management systems — Requirements," 2005.

[21] A. Martins and J. Eloff, “Assessing information security culture,” *Information security of South Africa (ISSA)*, Johannesburg: 2002.

[22] L. Ngo, W. Zhou, A. Chonka, and J. Singh, “Assessing the Level of I.T. Security Culture Improvement : Results from Three Australian SMEs,” *35th Annual Conference of IEEE Industrial Electronics (IECON),*, 2009, pp. 3189-3195.

[23] T. Gebrasilase and L. Lessa, “Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital,” *October*, vol. 3, 2011.

[24] T. Schlienger and S. Teufel, “Tool Supported Management of Information Security Culture,” *Security and Privacy in the Age of Ubiquitous Computing*, R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura, eds., Springer Boston, 2005, pp. 65-77.

[25] J. Finch, S. Furnell, and P. Dowland, “Assessing IT Security Culture: System Administrator and End-User Perspectives,” *Proceedings of ISOneWorld 2003*, 2003.

[26] A. Martins and J. Eloff, “Information security culture,” *In Security in the information society. IFIP/SEC 2002*, 2002.

[27] A. Da Veiga, N. Martins, and J. Eloff, “Information security culture – validation of an assessment instrument,” *Southern African Business Review*, vol. 11, 2007.

[28] E. Schein, *Organizational culture and leadership*, Jossey-Bass, 2004.