Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture

Completed Research Paper

Abiy Woretaw
Information Network Security Agency, Ethiopia
abiyworetaw@yahoo.com

Lemma Lessa
Addis Ababa university, Ethiopia
lemma.lessa@gmail.com

Solomon Negash
Kennesaw State University, USA
snegash@kennesaw.edu

Abstract

Information security is one of the most vital and demanding issues facing today's financial institutions such as banks. With widespread use of information technology and ever increasing connectedness to the global environment, financial institutions are increasingly exposed to wide-ranging threats. This research is aimed at assessing the existing information security culture in banks in Ethiopia with the intention to identify possible gaps that need management intervention. To that end, survey research method is employed that mainly uses quantitative data based on primary data collected from the headquarters of eleven banks in the capital Addis Ababa, Ethiopia. The study revealed that the level of information security culture in the banking sector in Ethiopia is unsatisfactory.

Keywords

Information security, information security culture, assessment, security risks, security threats

Introduction

The banking sector in Ethiopia is one of rapidly growing sectors of the country's economy. Many private banks are established in the past few years. The distribution and diversity of services is widening. Banking business competition has stirred the advancement of services enabled by information technology. More banks in Ethiopia are implementing Core banking solutions in order to provide banking services from any of their branch offices. Though this technological advancement has facilitated business processes, much attention should be drawn to thwart illegal financial gain efforts of cyber criminals. The security of the banking information systems and critical financial data should be ensured. The banking sector is more sensitive to the issue of security as money is at stake and is lucrative target for malicious attackers.

The technical aspect of information security has been given more attention so far, but a more serious yet under-rated aspect of information security is the human aspect. In line with this, Mitnick et al (2002) pointed that technical methods of protecting information may be effective in their respective ways; however, many losses are not caused by faulty technology but rather by users of technology and faulty human behavior. Hence, people not only can be part of the problem, but also they can and should be part of the solution. People must be integral part of any organization's information security defense system (Mitnick et al, 2002; Tanrıverdi & Metin, 2017). In support of this argument, Martins and Eloff (2006) underline that the behavior of employees and their interaction with computer systems have significant impact on the security of information.

Evolving trends in information security highly demand the incorporation of the human element in ensuring information security of an organization (Martins and Eloff, 2006; Vaast, 2007; Tu & Yuan, 2014; Kosutic and, 2018). Thus, assessing the level of existing information security culture provides clear picture in finding the gaps to intervene with managerial measures to promote sustainable information security culture. Such a strong information security culture within an organization also serves as a suitable platform to implement technical information security controls. Moreover, in order to promote a strong information security culture, the existing information security beliefs and practices should first be assessed so that critical gaps and possible areas of improvement are identified to pave the way for policy and management intervention.

Hence, this research is aimed at assessing the perception, attitude and practice of employees towards information security in the banking sector in Ethiopia; identify possible gaps to pave the way for policy and management intervention; and recommend measures that can be implemented by practitioners to enhance the information security culture in the banking sector in the country.

In the next section, brief literature review is presented on main issues of information security culture. Then description of the research method employed in the research is presented followed by details on the findings and discussions of the study. Finally conclusions drawn from the study as well as possible recommendations for future action are provided.

Literature Review

Information Security Culture (ISC)

Martins and Eloff (2006) define information security culture as the assumption about acceptable information security behavior and it can be regarded as a set of information security characteristics such as integrity and availability of information. Most of the recent researches approach information security culture from theories and models of organizational culture. Organizational culture defines how an employee perceives the organization. According to Schlienger & Teufel (2003), information security culture can be treated as a subculture with regard to general organizational culture.

Users can be either security asset or exploitable security weak-links for an organization. Hence it is critical that all people who interact with the information system exercise an acceptable information security culture. It is therefore fundamental to understand and manage the psychology of users so that their belief, perception and attitude towards information security is acceptable.

According to Schlienger & Teufel (2002), Security culture covers social, cultural and ethical measures to improve the security relevant behavior of the organizational members and considered to be a subculture of organizational culture. Thus it tends to be stable and resistant to change regardless of the security level it guarantees. Information security culture deals with the psychology and behavior of employees in their interaction with the information system. Reliable security culture assists the enforcement of information security policies and practices to the organization (Alnatheer & Nelson, 2009; Dincelli & Goel, 2018). As a result, each organization's goal should be to achieve a strong and sustainable information security culture.

Approaches to Organizational Information Security Culture

Studies have shown that technical solutions alone are not enough to manage internal security incidents. In order to have better security precautions in organizations, both the technical and non-technical aspects of information security need to be addressed (Zakaria et al, 2007). Zakaria et al (2007) further emphasize the importance of management activities in order to establish appropriate information security culture within an organization. The roles of senior management, allocation of budget, assignment of dedicated function, participation of employees, the enforcement processes and the awareness program are information security tasks needed to establish/enhance ISC (Lim et al, 2009).

In their ISC assessment article, Martins and Eloff (2006) describe that "ISC assessment approach consists of an audit process where the perceptions, attitudes, opinions and actions of employees regarding information security can be determined. By analyzing this information, an organization can assess how employees perceive information security activities and which aspects concerning information security culture need attention." (p.5). Martins and Eloff (2006) approach the information security culture audit

process by designing ISC questionnaire, actual survey process, data analysis and interpretations and recommendation phases. This approach is adopted by this research to assess the information security culture in the banking sector in Ethiopia.

Factors that Influence Information Security Culture and Practices

Alnatheer & Nelson (2009) classified factors that influence security culture and practices into four themes. Corporate citizenship which is achieved by information security awareness and training programs; Legal regulatory environment which deals with information security management standardization, best practices and information security policy; Corporate governance including top management support for information security management, information security compliance and information security risk analysis and Cultural factors like national and organizational culture.

Information Security Culture Model

A popular comprehensive model, Information Security Culture model designed by A. Martins and J. Eloff (2002), is derived from the organizational behavior model of Robbins (1989). This conceptual information security culture model is derived from the paradigm of approaching information security culture as a sub-culture of organizational culture. Martins and Eloff identified information security controls at individual, group and organizational levels of organizational behavior that could influence information security culture (N. Martins & J. Eloff 2002; A. da Veiga et al 2007).

This research assesses the level of information security culture in the banking sector in Ethiopia explicitly from the perspective of this model. The interrelationships between information security culture tasks (dependent and independent variables) at all levels are apparent from Figure 1.

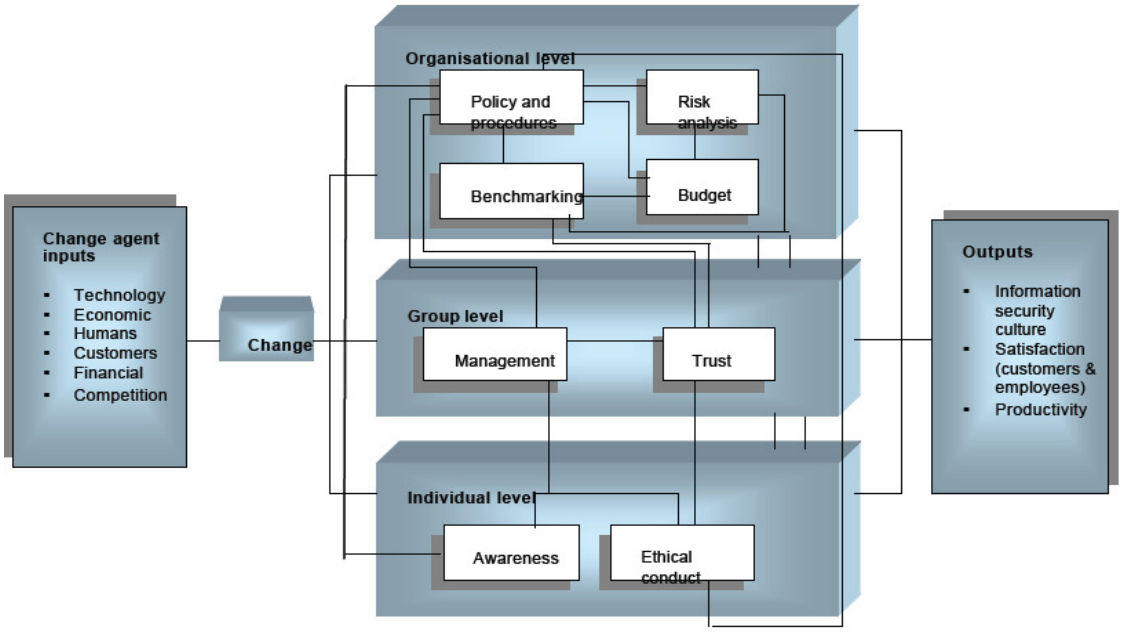

Figure 1. Adopted Information Security Culture Model Originally Developed by Martins & Eloff (2002).

Research Methodology

Study Design

A survey research method is employed in order to assess the information security culture in the banking sector in Ethiopia. This research is based on a widely accepted information security culture model originally developed by Martins A. and J. Eloff (2002). This research relied on quantitative primary data collected through a questionnaire developed based on a model to assess information security culture.

Instrument of Data Collection

Primary data is collected from headquarters of 11 different banks in Addis Ababa. A questionnaire to assess information security culture, developed by (Martins, 2002), is adopted. This assessment instrument is validated and improved by performing a factor and reliability analysis on the data from an information security culture assessment in a financial organization (Veiga et al, 2007). Factors in the establishment and maintenance of proper information security culture are assessed. Then information security culture in the banking sector in Ethiopia is evaluated by auditing process.

The questionnaire has 41 statements that assess the perceptions, attitudes, opinions and actions of employees regarding information security. A five point Likert scale, which is advisable to assess behavioral patterns, is provided to respond to the information security culture statements. Minor changes were made to contextualize the questionnaire to the target research participants.

Subjects and Sampling

Total of eleven banks (2/3rd of all banks in Ethiopia) participated in the research. Four of these banks are state-owned (Commercial Bank of Ethiopia (CBE), National Bank of Ethiopia (NBE), Construction and Business Bank (CBB) and Development Bank of Ethiopia (DBE)). The remaining seven private banks are: Lion International Bank (LIB), Dashen Bank, Wegagen Bank, Bank of Abyssinia, Awash International Bank (AIB), Zemen Bank and Oromia International Bank (OIB). The survey is conducted at headquarters of these banks located at different sites in Addis Ababa. An assumption is made that information security culture in branch banks bear resemblance to the information security culture practiced at headquarters. A non-probability convenience snowball sampling technique is used to collect data from all the banks. The general objective is communicated to contact-persons in all the 11 banks and they steward the data collection. This sampling technique capitalizes on insider experience and so facilitates the data collection process.

Bank employees in the IT or Information Systems (IS) departments are the main respondents of the survey because these employees directly access the banks' valuable and confidential information systems. In addition to this, IT departments serve as a liaison between the managerial and operational staffs. Furthermore, these employees are assumed to have the minimum information security awareness required to complete the questionnaire. This aids the respondents to perceive the meaning of the statements uniformly. IT professionals, departmental managers and operational staffs of IS/IT department are subjects of this research. The trend with these employees is assumed to heavily influence the information security culture of other departments. Thus, assessing the level of information security culture in IS/IT departments substantiate the findings of the research because the subjects are at the heart of the banks' information systems. Hence, conclusions and recommendations made based on research findings from these subjects' data are believed to be valid and reliable.

Data Analysis and Discussion

In order to effectively analyze the collected data based on the information security culture model, the 41 information security culture statements are categorized into four groups [individual level, group level, organizational level and change] dimensions.

Individual Level Dimension includes two sub-dimensions called Awareness and Ethical conduct. Awareness sub-dimension statements assess the knowledge, attitude and perception of employees towards information security. Ethical conduct sub-dimension statements assess the adherence of

employees to existing information security policy and procedures and their perception towards access to data and intellectual property. The management regard to privacy of employees' information is also considered in this sub-dimension.

Group Level Dimension includes two sub-dimensions named Management and Trust. Management sub-dimension statements assess the perception and commitment of top management to information security. The establishment of a dedicated information security function in the banks, communication of security information on a need-to-know basis and participation of employees in information security initiatives are also assessed in this sub dimension. Trust sub-dimension statements assess the trust environment between employees and their managers at different levels.

Organizational Level Dimension includes four sub-dimensions named Risk analysis, Policies and procedures, Benchmarking and Budget. Risk analysis sub-dimension statements assess the availability of dedicated risk analysis function and perception of employees about the importance of risk analysis in the bank. Policies and procedures sub-dimension statements assess whether the bank has implemented information security plan, policy and procedures. Availability of formal information security incident reporting procedures and access of employees to all these documents is also evaluated. Benchmarking sub-dimension statements assess the evaluation of the bank's information security status compared with other banks and its compliance with international standards. Budget sub-dimension statements assess the perception of employees about the importance of budgeting annually for information security as a strategic investment.

Change Sub-Dimension statements assess the readiness and acceptance of employees to new information security practices and the recognition and organization of the bank's management to information security changes.

Findings of the Survey

The information security culture data is collected from 4(37%) state-owned and 7(63%) private banks. The job category distribution of the respondents indicates 12 (12%) department managers, 58(58%) IT professionals, 18 (18%) operational staffs and the remaining 12(12%) respondents did not complete this variable. With regard to the years of experience, all experience levels of employees in the banking sector in Ethiopia are represented. 19(19%) of the respondents have more than 10 years of experience in the banking sector. 22(22%) of the respondents have 5 to 10 years of experience. 28(28%) of the respondents have 2 to 5 years of experience.23(23%) of the respondents have less than 2 years of experience in the banking sector. The remaining 8(8%) did not respond to this variable. Generally, the information security culture level in the banking sector in Ethiopia is found to be inadequate. Only 25% of the respondents are found to have favorable information security culture [>=32/41]. The remaining 75% have unfavorable information security culture that can expose the information asset of the banks. This shows that holistic and strategic work is needed to promote information security culture in the banking sector in Ethiopia.

Figure 2 represents the percentage of respondents who are found favorable and unfavorable about the statements portrayed in the four dimensions of information security culture. The favorable percentages indicate the information security perception, attitude and behavior in the banks that are in line with strong information security culture. The unfavorable percentages indicate the information security perception, attitude and behavior gaps that are possible improvement areas. Larger unfavorable percentage indicates wider gap in the variable of interest that needs serious managerial intervention. From figure 2, it is evident that individual, group and change dimensions are critical developmental areas. The organizational level information security culture dimension scores a slightly better (38%) result.

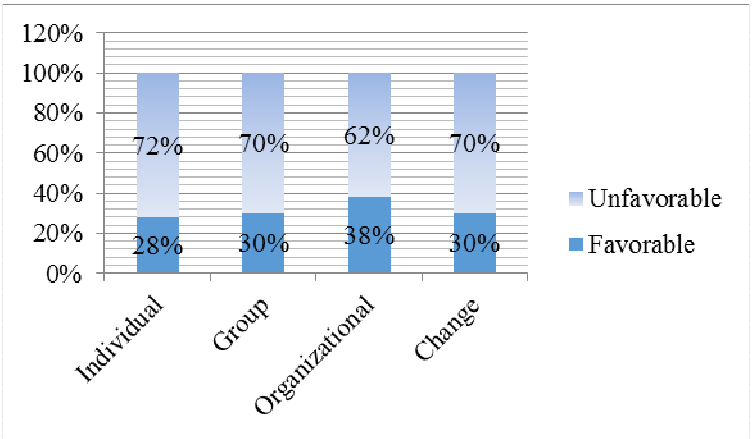

Figure 2. Information Security Culture Dimensions Assessment Result

Figure 3 represents the percentage of respondents who are found favorable and unfavorable about the statements portrayed in the nine sub-dimensions. The frequency distributions of the nine sub-dimensions indicate that ethical conduct, trust, benchmarking, policy and procedures, and change are developmental sub-dimensions that need serious managerial attention. Nevertheless, frequency distributions of awareness, management, budget and risk analysis sub-dimensions show average results that also need significant improvement.

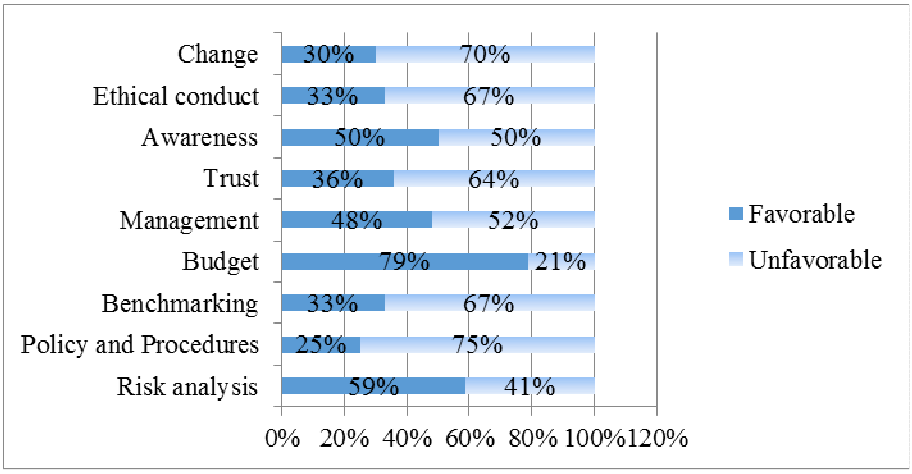

Figure 3. Information Security Culture Sub-Dimensions Assessment Result

Risk Analysis Sub-Dimension of ISC

Respondents perceive the importance to perform risk analysis positively (94%). However only 60% of the respondents believe there is a function responsible for risk analysis of information assets in the banks. This implies risk analysis is not conducted formally and imminent information security threats might not be communicated to employees. Every bank should clearly dedicate a function that effectively conducts risk analysis of information assets in the bank.

Policy and Procedures Sub-Dimension of ISC

Formal information security incident reporting procedures (32%) suffer a negative result in the banking sector in Ethiopia. This is partly because security incident reporting procedures are not developed or not effectively disseminated to employees. Access to information security policy and procedures also suffers a poor 33% frequency distribution. The implementation of information security procedures (48%) is not at satisfactory level as security should be approached holistically. Security compromise at one level can mean compromise at every level. Even the relatively better information security plan (65%) is not satisfactory taking the security sensitivity of the banking sector into consideration. Banks in Ethiopia should develop formal procedures indicating how employees report information security incidents. The dissemination and implementation of the information security policies also need serious attention.

Benchmarking Sub-Dimension of ISC

Respondents negatively perceive the compliance of the banks information security measures with international standards (28%). Most respondents are not sure about the level of information security practice compared with other banks. Continuous information security evaluation (58%) also needs to improve. Vulnerability assessment and auditing should be conducted on a continuous basis. Banks in Ethiopia should cooperate to share information security incidents and best practices. Benchmarking international standards can also benefit banks to succeed objective results. International information security standards like code of practice for information security: ISO27002 and specification for an information security management system: ISO27001 should be implemented at organizational level to assist the establishment of reliable information security culture. Compliance with these international standards assists in promoting positive information security culture.

Budget Sub-Dimension of ISC

Respondents perceive budgeting annually for information security costs is a strategic investment. This attitude is considered positive to promote the information security change initiatives. This sub-dimension enjoys the highest overall result (79%). However it is worth noting if the budgeting practice in the banks does not match the perception about budgeting, the result can be misleading. If top management of the banking sector in Ethiopia does not practically back the positive budgeting endorsement by employees, this sub-dimension result will be unrealistic. However the fact that information security budgeting is perceived positively indicates information security initiatives are positively endorsed by employees. This provides a suitable ground to participate and delegate information security tasks to employees.

Management Sub-Dimension of ISC

The management sub-dimension is averagely perceived by the respondents. Even though employees generally know the function responsible for information security in the bank (77%), the managers' involvement in communication, implementation and harnessing employees' participation should be improved. Respondents perceive the understanding (60%) and support (62%) of top management to information security implementation inadequately. The participation of employees in decision making is 62%. However the communication of security information on a need-to-know basis to employees (45%) is perceived negatively. Thus, management should communicate information security procedures and guidelines to all job levels on a need-to-know basis.

Trust Sub-Dimension of ISC

The trust relationship between employees and their immediate managers is found relatively positive than that of employees and top management. So top management should sometimes directly approach and communicate with employees to build a positive trust environment at all levels.

Awareness Sub-Dimension of ISC

The perception of respondents about the importance of information security is positive. However, training employees in information security controls and measures they are supposed to use (52%) is the lowest score in the Awareness sub-dimension. This shows if information security trainings are provided to

employees, banks can further enhance the level of information security awareness perception, attitude and knowledge of their employees. The training program should be designed based on the output of the information security risk analysis and information security policies and procedures.

Ethical Conduct Sub-Dimension of ISC

The information access perception of employees (44%) needs attention as it contributes to unintentional compromise of information asset by insiders. Information access within the bank has to be limited on a need-to-know basis. The adherence of employees with the banks' information security policy is only partially (50%) ensured by banks. This auditing measure is also a critical improvement area.

Change Sub-Dimension of ISC

The readiness (83%) and acceptance (73%) of employees to change their information security practices is positive. However the perception towards organization (42%) and recognition (47%) management of information security changes is found to be unsatisfactory in the banking sector in Ethiopia. Hence, positive information security changes should be recognized and rewarded while non-adherence should bear accountability measures. Bank managers should also oversee and recognize the impact of positive information security culture change.

Discussion of Results: Interrelationship between the ISC Sub-Dimensions

Binary logistic regression is computed between dependent and independent variables [Adjusted Odds Ratio (95% CI) = the odds ratio (lower limit of the confidence interval, upper limit of the confidence interval)]. The probability of an increase in dependent variable influenced by increase in independent variable can be portrayed with adjusted odds ratio with lower and upper limits of the confidence interval. The results are interpreted from the perspective of the information security culture conceptual model and related literature review. Then conclusions and recommendations are framed based on the statistical findings and interdependence between information security culture sub-dimensions.

As per the results from the computed binary logistic regression, the likelihood of effective implementation of information security policies and procedures due to suitable ethical conduct is positive [AOR (95% CI) = 6.065 (2.278, 16.150)]1. This signifies attention should be drawn to enhance the ethical conduct, willingness to adhere with information security policy and guidelines, of employees. The role of management to promote information security awareness is observed imperative [AOR (95% CI) = 2.667 (1.188, 5.985)].This implies that improving the information security awareness of managers influence the overall information security awareness of the bank. Awareness and ethical conduct are information security culture tasks an organization has to enhance in order to advance individual level information security practices. The prevalence of acceptable individual level information security culture in assisting positive change of information security culture in the banks is also observed from the data analysis [AOR (95% CI) = 2.581 (1.036, 6.428)].

Management attributes such as communication of security information on a need-to-know basis and participation of employees in information security initiatives most likely raise a positive trust environment in the banks [AOR (95% CI) = 4.964 (2.032, 12.127)]. Positive trust environment is observed to maintain effective implementation of information security policies and procedures [AOR (95% CI) = 3.066 (1.206, 7.795)]. The role of management in effective implementation of information security policies and procedures is essential [AOR (95% CI) = 5.023 (1.795, 14.053)]. Management and trust are information security factors that constitute group level information security culture. Proper accommodation of group level information security culture tasks encourages the readiness and acceptance of employees to change their information security practices that results in positive information security culture change [AOR (95% CI) = 4.571 (1.811, 11.540)].

Policy and procedures are found to coexist with risk analysis [AOR (95% CI) = 5.112 (1.601, 16.325)]. Benchmarking tasks such as information security evaluation and compliance with international standards

[1] [Adjusted Odds Ratio (95% CI) = the odds ratio (lower limit of the confidence interval, upper limit of the confidence interval)].

could only be expected if the bank implements information security policies and procedures [AOR (95% CI) = 7.836 (2.866, 21.421)]. These organizational level information security culture tasks; risk analysis, policy and procedures and benchmarking impact the recognition and management of positive information security change in the banking sector in Ethiopia[AOR (95% CI) = 5.778 (2.281, 14.633)]. Regardless of the other organizational level sub-dimensions, Budget sub-dimension is found to have no association with any of the other eight sub-dimensions. This is probably because the result of the benchmarking sub-dimension (79%) doesn't align with other findings. If the statements assessed the allocated budget rather than the perception of employees about the importance of budgeting, the result would have been different and association could have been observed with other sub-dimensions.

In line with the information security culture model employed, the information security culture tasks at different levels are statistically analyzed to be interrelated. Organizational level information security culture tasks are built upon individual and group level information security tasks. The likelihood of individual information security culture endorsing organizational information security culture is [AOR (95% CI) = 4.173 (1.678, 10.377)]. The interdependence between group and organizational level information security culture tasks is also apparent from the computed binary logistic regression [AOR (95% CI) = 7.275 (2.805, 18.866)]. These findings further validate the model adopted is feasible to assess the information security culture in the context of the banking sector.

The culmination of all the three levels of information security culture tasks result in cultivating a positive information security culture change. It is essential to identify, prioritize and deal with developmental information security culture elements. Identifying the causal link between the information security culture sub-dimensions helps in finding a strategic way to prioritize and invest on information security initiatives. The statistical frequency findings point out the gaps underlying in the existing information security culture in the banking sector in Ethiopia. Integration of statistical frequency findings with association between interdependent sub-dimensions provides a clear understanding that directs effective engagement measures to promote information security culture in the banking sector in Ethiopia.

Conclusion

This research assessed the level of existing information security culture in the banking sector in Ethiopia. It employed quantitative method based on a validated information security culture questionnaire from previous related literature. The collected data is analyzed with respect to well established factors that influence information security culture. The study revealed that the information security awareness in the banking sector in Ethiopia is unsatisfactory. This possibly emanates from inadequate information security communication and training. There is also a significant space to enhance the trust environment between managers and employees that can promote change in information security culture. Consequently, the level of proper information security governance in the banking sector in Ethiopia is a critical area of improvement. Hence, we strongly recommend that banks in Ethiopia should invest in effective information security communication methods like training employees with information security measures and information security policy awareness programs. International information security governance standards like ISO27002 and information security management standards like ISO27001 should be implemented at organizational level to assist the establishment of reliable information security culture. Compliance with these international standards ensures moving in the right direction.

Information security initiatives should be championed by top management to boost the implementation of information security policies. A dedicated team should be responsible to manage the initiatives and participation of all employees in the bank should be fostered to effectively embrace positive information security culture change. Research on information security culture is still in its early stages of development. Issues are still being identified, and, conceptualizations being explored (Alnatheer & Nelson, 2009; Gebrasilase & Lessa, 2011). This hot research area is even at its infant stage in Ethiopian banking sector context. This paper tried to bridge the gap in researching the information security culture in the banking sector in Ethiopia. However, it suffers limitations in incorporating all departments in the banks with larger sample size. Therefore, more rigorous researches are needed to frame practical strategies to enhance the information security culture in the banking sector in Ethiopia.

Limitation of the Study

The scope of this research is assessing the level of information security culture in the banking sector in Ethiopia. The subjects of the study are mostly employees and managers of Information Systems department from 11 headquarters of banks in Ethiopia. A more inclusive survey of other departments would have made the research findings more comprehensive. The survey and model are based on a 2002 study that did not rigorously explain its scale development steps. For that reason, and due to the dynamic environment of IT, it is critical to thoroughly assess the reliability and validity of previously used scales. Besides, we have considered sample of 100 and a higher sample size may give more power.

References

Alnatheer, M. & Nelson, K. (2009) A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context, Australian Information Security Management Conference: Security Research Centre Conferences, 5-17.

Dincelli, E. and Goel, S. (2018) Understanding Nuances of Privacy and security in the context of Inofrmation Systems, 10-12 August, Boston, Massachusetts, USA.

Kosutic, D. and Pigni, F. (2018) Exploring the Impact of Information Security Practices on Competitive Advantage; Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018.

Lim, J. S., Chang, S., Maynard, S. B. & Ahmad, A. (2009) Embedding information security culture emerging concerns and challenges, Proceedings of the 7th Australian Information Security Management Conference, 463-474.

Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009) Exploring the Relationship between Organizational Culture and Information Security Culture, In 7th Australian Information Security Management Conference, SECAU Security Congress 2009, 87-97.

Martins, A. & Eloff, J. (2002) Assessing Information Security Culture, Information Security South Africa (ISSA), Johannesburg, South Africa, 1-12.

Martins, A. (2002) Information security culture, MCom Thesis, Rand Afrikaans University.

Robbins, S. P. (1989) (ed.) Organizational Behavior: Concepts, Controversies, and Applications. New Jersey: Prentice Hall.

Schlienger, T. & Teufel, S. (2002) Information Security Culture: The Socio-Cultural Dimension in Information Security Management, in Proceedings of 17th International Conference on Information Security (SEC2002), 214: 191-202.

Schlienger,T. & Teufel, S. (2003) Information security culture – from analysis to change, Proceedings of the 3rd Annual Information Security South Africa Conference, Information Security South Africa (ISSA), Johannesburg, South Africa, 2003: 183–196.

Tanrıverdi, N. and Metin, B. (2017) Evaluation of IT Security Perception; Twenty-third Americas Conference on Information Systems, 10-12 August, Boston, Massachusetts, USA.

Tu, Z. and Yuan, Y. (2014) Critical Success Factors Analysis on Effective Information Security Management: A Literature Review; Twentieth Americas Conference on Information Systems, August 7-10, Savannah, GA.

Vaast, E. (2007) Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. Journal of Strategic Information Systems 16 (2007), 130–152.

Van Niekerk, J., & Von Solms, R. (2006) Understanding Information Security Culture: A Conceptual Framework, Information Security South Africa (ISSA), Johannesburg, South Africa.

Van Niekerk, J. F., & Von Solms, R. (2009) Information Security Culture: A Management Perspective, Computers & Security, In Press, Corrected Proof.

Veiga, A. D., Martins, N. & Eloff J.H.P. (2007) Information security Culture- validation of an assessment instrument, Southern African Business Review, 11(1): 147-166.

Veiga, A. D., & Eloff, J. H. P. (2010) A Framework and Assessment Instrument for Information Security Culture, Computers & Security, 29(2): 196-207.

Von Solms, S. H. (2000) Information Security- The Third Wave?, Computer & Security, 19: 615-620.

Zakaria, O., Gani, A. et.al (2007) Reengineering Information Security Culture Formulation Through Management Perspective, In Proceedings of the International Conference on Electrical Engineering and Informatics Institute, Indonesia.