ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 8, Issue 3, pp: (319-328), Month: July - September 2020, Available at: www.researchpublish.com

INFLUENCE OF STAFF TRAINING AND AWARENESS ON CYBERSECURITY READINESS IN DEPOSIT-TAKING SAVINGS AND CREDIT COOPERATIVE ORGANIZATIONS IN KENYA

Nancy Nyawira Muraguri[1], Tobias Mwalili[2], Thomas Mose[3]

[1](Department of Information Communication Technology, College of Human Resource Development, Jomo Kenyatta University of Agriculture and Technology, Kenya)

[2](Department of Information Communication Technology, College of Human Resource Development, Jomo Kenyatta University of Agriculture and Technology, Kenya)

[3](Department of Information Communication Technology, College of Human Resource Development, Jomo Kenyatta University of Agriculture and Technology, Kenya)

Abstract: **The purpose of carrying out this study was to establish the influence of staff training and awareness on cybersecurity readiness in deposit-taking savings and credit cooperative organizations in Kenya. This study focused on SACCOs within Nairobi County and the target population was the 40 deposit-taking SACCOs in Nairobi County. Respondents were obtained from the ICT department, top management, and customer service department of the SACCOs, the selection of the respondents was done randomly. The instruments that were used were self-administered questionnaires and a census of all the SACCOs was conducted. Secondary data was obtained from SASRA's reports and other relevant publications in referred journals. The collected data was coded and analyzed quantitatively (frequencies and percentages) as well as statistical inferential (regression analysis). This study also used the Pearson correlation and analysis of variance (ANOVA) to determine whether the independent variables had a combined effect on the dependent variable. The analyzed data was presented in tables, findings discussed, conclusions drawn, and policy implications outlined. The findings of the study revealed that there is a positive and significant correlation between staff training and cybersecurity readiness. The study also concluded that effective training programs aimed to enlighten the staff on cybersecurity issues are an important ingredient for cybersecurity readiness in deposit-taking SACCOs. The study recommended that more training programs are organized regularly to enhance cybersecurity readiness.**

Keywords: **Staff Training, Awareness, Cybersecurity Awareness and Deposit Taking Savings.**

1. INTRODUCTION

Savings and Credit Cooperative Societies (SACCOs) are voluntary financial institutions owned and controlled by their members and operated for the purpose of providing credit at low-interest rates, promoting savings and providing other non-financial services to its members (Waweru, 2011). Today SACCOs are one of the largest financial institutions addressing the needs of all people from different backgrounds (FAO, 2018). The first SACCO in Kenya was Lumbwa cooperative which was formed by European farmers in 1908 with the goal of supporting agricultural activities and products to take advantage of economies of scale (Ministry of industry, trade, and Cooperatives, 2014).

The first cooperatives were registered as companies and only became registered as co-operatives in 1931 when the first co-operative was promulgated and they were predominantly marketing oriented and auxiliary focused (Ministry of industry, trade, and cooperatives, 2014). By 1999 more than seven thousand cooperatives had been registered in Kenya. In recognition of the growing importance and sophistication of SACCOs, a SACCO Societies' Act was enacted in 2008 to pave way for vigorous enforcement of prudential standards for SACCOs with front office services activities (FOSAs). This gave rise to the SACCO Regulatory Authority (SASRA) the body charged with the responsibility of regulating deposit-taking SACCOs (Ministry of industry trade and cooperatives, 2014). Information Communication and Technology (ICT) drives businesses in a fast-paced world, where customer satisfaction and competitiveness are measured by convenience, speed of service delivery, efficiency, and cost-effectiveness (Cumby, 2006). Financial institutions have also been revolutionized by ICT especially the internet through electronic financing. Gary (2006) insisted that SACCOs must turn to e-marketing in order to cope with the current demand to meet the client's expectations and establish long-lasting relationships with their customers. By integrating ICT into their business strategies SACCOs can improve acquisition and retention of customers.

Cybersecurity is the collective application of strategies, security measures, threats administration tactics, training, paramount practices, assurance and expertise that can be used to guard the information system, organization and all related assets (International Communication Union, 2004). Cybersecurity readiness refers to the ability of an organization to detect and effectively respond to computer security intrusions and breaches, theft of data and intellectual property, phishing attacks, and malware attacks from both outside and inside the network (Sullivan, 2016). As cited by Richmond (2017) organizations need not worry about when they will be breached but rather whether they are adequately prepared to detect attacks, quickly recognize a breach, effectively remediate and accurately assess the damage. Cybersecurity readiness shows an organization's behaviors, practices, and processes towards managing risk, having efficient cybersecurity controls, training employees on cyber risks and detecting and responding to threats.

Cybersecurity ventures (2019) predicted that cybercrime will cost the world a surplus of 6 trillion US dollars by the year 2021 up from the 3 trillion US dollars cybercrime costs incurred in 2015. Cybercrime costs include lost productivity, stolen money, disruption to businesses, forensic investigation, intellectual property theft, restoration of hacked systems and reputation harm. Most organizations acknowledge that they are unlikely to spend more money or their cybersecurity practices unless they suffered a breach or an incident that would cause negative impacts to the organization (E&Y, 2018). Organizations worldwide are struggling to understand and manage emerging cyber risks in a sophisticated digital society. Information Technology (IT) analysts within organizations are still unable to keep up with the pace of the dramatic increase in cybercrime and sophisticated attacks on their networks. More than 90 percent of successful data breaches and hacks originated from phishing emails that were designed to entice recipients to open a document or click a link. Organizations need to be aware that there is no one size fits all type of security technology and that they need to overlap security processes to improve their organization's security culture in order to better secure their systems. Organizations need to plan for cyberattack in order to ensure that they can prevent most breaches and respond more promptly when an attack occurs (Cybersecurity ventures, 2019). Credit unions which are like SACCOs in Kenya are a growing target for cyber-attacks. Breaches of these institutions rarely make the news; however, attacks are growing at a high frequency. These institutions fail to match advanced security technologies and they also fail to observe the appropriate security practices this hence leaves their entry points exposed. Most organizations have adopted complex environments and increasingly use cloud-based applications, hybrid IT infrastructure, the increase in the use of these applications has introduced vulnerabilities and weak links which have exposed organizations data.

2. STATEMENT OF THE PROBLEM

Increased organizational dependence on ICT has led to a corresponding increase in the effect of ICT security abuses (Kankanhalli *et al.*, 2003). SACCOs have become an easy target to cyber-attacks such as malware attacks, ransomware attacks, data breaches, abuse of privileged access, critical data manipulation and email phishing attacks. Despite warnings of the increase in the number of threats afflicting organizations seventy-three percent of organizations face major drawbacks in terms of cybersecurity readiness (Hiscox, 2018). Serianu (2018) found out that majority of the SACCOs in Kenya are underprepared for the surge in new sophisticated malware and advanced persistent threats (APTs). SACCOs continue to fall victim of a variety of cyber-attacks; malware infections, crypto-jacking, banking trojans such as emotet, denial of service, ransomware, social engineering, and phishing scams.

The number of SACCOs that have fallen prey to cybercriminals has increased (Mwitari, 2018). These cybercriminals either act as alone or with malicious employees within the SACCO. The effects of these attacks include financial losses, a decline in market share, loss of reputation and customer trust (Reid, 2018). Very few studies have been done in the context of cybersecurity readiness in deposit-taking SACCOs in Kenya. This study sought to establish the influence of staff training and awareness on cybersecurity readiness in deposit-taking savings and credit cooperative organizations in Kenya.

3. LITERATURE REVIEW

Organizations that are keen on securing their systems and are keen on ensuring they can detect and respond to cyber-attacks by empowering their employees. Organizations need to view cybersecurity holistically and ensure that top management executives and employees are actively involved in security issues and ensure that everyone understands cybersecurity risks and most crucially every employee knows the specific steps to mitigate these risks. Prevention of cyber-attacks starts with training employees to recognize and respond to hacking attempts such as phishing and social engineering. The provision of professional training to ICT staff will empower them on how to protect critical infrastructure, implementing security controls and how to detect vulnerabilities within the organization. User awareness of cybersecurity risks and threats can empower users on best practices to better protect themselves online thereby improving the security posture of an organization (D'Arcy, 2008).

The human factor is a major factor of cybersecurity. Changing user behavior changes the organization's security culture. According to ACS (2018), staff training and awareness is a key pillar of cybersecurity readiness, individuals can be an attack vector through social engineering and everybody within an organization should be responsible for ensuring that cybersecurity best practices are carried out. Staff education should be done regularly and materials should be updated as new threats arise. Employees have been identified as an important factor empowering cybersecurity within the organization because security incidents most often are the result of employees' lack of awareness of the organization's information security policies and procedures (Hansche, 2002; Mitnick, 2003). Ponemon Institute (2012) conducted a study on the state of small business's cybersecurity readiness in the United Kingdom. The study recognized compliance to regulations and laws was critical for the small businesses that were surveyed; the study also found out that one of the barriers to achieving cybersecurity readiness in those organizations was lack of in-house skilled staff or expert personnel.

Aloul (2012) noted that phishing attacks in the United Arab Emirates (UAE) were on the rise, he noted that many individuals fall for phishing scams due to the lack of knowledge on how to recognize a phishing email, this, therefore, puts the organization's data at risk. He suggested that general user education was an important approach to fight phishing scams. Catota *et al*., (2018) established that the barriers that prevent Ecuadorian financial institutions from properly responding to security incidences include the lack of awareness and training. They suggested that executive managers need to be educated about observing security; they need to be made aware of the policies guiding the use of their own personal devices within the corporate network. Jaatun *et al*., (2007) found out that personnel involved in project implementation focused too much on the technology at the expense of human factors, the researchers found out that failure to promptly detect and respond to cybersecurity incidences was due to the lack of situational awareness of various virus threats and lack of scenario training on handling virus and worms attacks within the organizations.

Musuva *et al*., (2015) found out that one of the gaps in cybersecurity was employee training and awareness and technical training of technical personnel. They noted that most technical staff within organizations combined cybersecurity roles with IT roles, these individuals are overloaded with other tasks within the organization and lack the necessary skill set to handle cybersecurity incidents. They also found out that the consequence of a lack of employee training was that the organizations were not cyber prepared to deal with cybersecurity incidences. The researcher, therefore, intended to determine how training and awareness of information security risks influences cybersecurity readiness in SACCOs.

4. RESEARCH METHODOLOGY

This study focused on SACCOs within Nairobi County and the target population was the 40 deposit-taking SACCOs in Nairobi County. Respondents were obtained from the ICT department, top management, and customer service despartment of the SACCOs, the selection of the respondents was done randomly. The instruments that were used were self-administered questionnaires and a census of all the SACCOs was conducted. Secondary data was be obtained from SASRA's reports and other relevant publications in referred journals. The collected data was coded and analyzed

quantitatively (frequencies and percentages) as well as statistical inferential (regression analysis). This study also used the Pearson correlation and analysis of variance (ANOVA) to determine whether the independent variables had a combined effect on the dependent variable. The analyzed data was presented in tables, findings discussed, conclusions drawn, and policy implications outlined.

5. FINDINGS

The focus of this study was to determine the influence of staff training and awareness on cybersecurity readiness in deposit-taking SACCOs. The study further sought to establish whether ICT security is handled by in-house employees or whether the organizations outsource cybersecurity services. The results are presented in Table 1.

The study aimed at finding out whether the organization's had employees on site or whether they had outsourced their cybersecurity operations.

Table 1: Employees who handle ICT security

ICT security staff	Frequency	Percentage
In house employees	63	63
Partly Outsourced	37	37
Completely outsourced	0	0
Total	**100**	**100**

The findings revealed that 63% of the SACCOs, had an employee on-site within the organization that could address the incidences in the event of a cyberattack. The findings also disclosed that 37% of the SACCO's ICT security is handled by partly outsourced employees. The study further disclosed that none of the organizations had completely outsourced their cybersecurity operations.

The study further sought to establish the number of respondents who have attended any training, workshop or awareness sessions in relation to cybersecurity organized by the SACCO. The results are presented in Table 2.

Table 2: Training Attendance

Training Attendance	Frequency	Percentage
Yes	44	44
No	56	56
Total	**100**	**100**

The findings revealed that the majority of the respondents (56%) had not attended any training, workshop or awareness sessions in relation to cybersecurity organized by the SACCO. However, 44% of the respondents indicated that they have attended some training and awareness sessions that were organized by their respective SACCOs.

The respondents who indicated they have ever attended training or awareness sessions were advised to indicate the last time they attended the session. The results are presented in Table 3.

Table 3: The last session attended

Last session	Frequency	Percentage
Within the last year	33	75
Within the last two years	11	25
Within the last three years	0	0
Total	**44**	**100**

The findings revealed that majority of the respondents who had attended training or awareness sessions did so within the last year as shown by 75%. The other (25%) had attended within the last two years. This implies that most of the SACCOs that train their employees do so annualy.

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 8, Issue 3, pp: (319-328), Month: July - September 2020, Available at: www.researchpublish.com

Table 4: Descriptive statistics for training

Statement	Strongly Agree (%)	Agree(%)	Undecided(%)	Disagree(%)	Strongly Disagree(%)	Mean	Standard Deviation
The Sacco trains us on Cybersecurity risks and threats and how to handle them	26	15	4	33	22	2.65	1.359
The Sacco trains us on Cybersecurity policies and best practices	21	12	4	56	7	2.84	1.339
The Sacco offers professional training opportunities to technical personnel	14	40	0	39	7	2.73	1.254
ICT staff within the SACCO have been trained on how to use and manage the security technologies within the organization	14	50	0	29	7	2.21	1.008
Aggregate scores						**2.61**	**1.24**

On the same note, 21% of the respondents agreed that their organization trains them on cybersecurity policies and best practices while 12% strongly agreed. However, quite a large proportion of the respondents were in disagreement as shown by 56% who disagreed and 7% who strongly disagreed that their SACCO trains them on cybersecurity policies and best practices. The majority of the respondents were in agreement that their respective SACCOs offer professional training opportunities to technical personnel as shown by 40% who agreed and 14% who strongly agreed. However, 39% of the respondents disagreed and 7% strongly disagreed.

The majority of the respondents were in agreement that ICT staff within their organization have been trained on how to use and manage the security technologies within the organization as shown by 50% who agreed and 14% who strongly agreed. On the other hand, 29% disagreed and 7% strongly disagreed. Besides, the study sought to establish the respondents, opinion on how influential the trainings are on cybersecurity readiness of the SACCO. The responses varied from one SACCO to another, but most of the respondents indicated that the training on cybersecurity has been very influential. Some of the respondents indicated that training and awareness sessions help staff to be aware of the threats posed by cybersecurity to the organization.

Some of the respondents cited that the trainings provide skills and knowledge that prepare the technical staff to handle any cybersecurity threats that they might have experienced. However, there are some of the respondents who indicated that training sessions need to be done frequently since security technologies are changing and new variants of malware are coming up each day.

Besides, the study sought to establish the respondents, opinion on how influential the trainings are on cybersecurity readiness of the SACCO. The responses varied from one SACCO to another, but most of the respondents indicated that the training on cybersecurity has been very influential. Some of the respondents indicated that training and awareness sessions help staff to be aware of the threats posed by cybersecurity to the organization. Some of the respondents cited that the trainings provide skills and knowledge that prepare the technical staff to handle any cybersecurity threats that they might have experienced. However, there are some of the respondents who indicated that training sessions need to be done frequently since security technologies are changing and new variants of malware are coming up each day.

The objective of the study was to determine the influence of staff training and awareness on cybersecurity readiness in deposit-taking SACCOs. The regression results revealed that there is a significant positive correlation between staff training and awareness on cybersecurity readiness at **β= 0.226; t = 2.146**; and **p = 0.004.** Therefore, staff training and awareness positively influences cybersecurity awareness; hence, an increase in staff training and awareness leads to an increased level of cybersecurity preparedness. The results of the regression equation revealed that a unit increase in staff training and awareness lead to a **0.226** increase on cybersecurity readiness. The findings support previous studies. ACS (2018), found that staff training and awareness is a key pillar of cybersecurity readiness. Hansche (2002) and Mitnick,

(2003) identified that employees are an important factor. Empowering staff on cybersecurity issues is key because security incidents most often are the result of employees' lack of awareness of cybersecurity best practices.

Human beings are considered to be weakest link in cybersecurity. Staff training and awareness is key in equipping employees with the knowledge they need to protect themselves from cybercrime elements such as social engineering. The findings of the study revealed that a high proportion of the SACCOs do not organize training and awareness sessions in relation to cybersecurity for their staff. However, those SACCOs that organize the training and awareness sessions do so annually. The study further revealed that most of the SACCOs do not train their staff on cybersecurity risks and threats as well as how they should handle various risks such as phishing attacks. The study also disclosed that some of the SACCOs do not train their employees on cybersecurity policies and bests practices while a few of them do.

The study found that most of the SACCOs offer professional training opportunities to their technical personnel, but quite a number of SACCOs do not. However, the majority of the SACCOs indicated that ICT staff within their SACCOs have been trained on how to use and manage the security technologies that have been implemented within the organization. Further, the results of regression and correlation analysis revealed that there is a positive and significant correlation between staff training and cybersecurity readiness. This implies that an increase in staff training leads to a significant increase in cybersecurity readiness. In fact, staff training was found to be the most significant variable in the study.

6. CONCLUSION AND RECOMMENDATION

Based on the findings of this study the research concluded staff training and awareness influences cybersecurity readiness in deposit taking SACCOs. Staff training was found to be most significant factor that influences cybersecurity readiness in SACCOs. The study further established that most of the staff were not trained this therefore acts as a loop hole for phishing attacks and social engineering. In the event an adversary decides to exploit this loop hole and sends and email attachment containing ransomware and an employee who has no proper training opens this attachment, this will in turn risk the organization's data being encrypted and critical systems such as servers will be inaccessible. Effective training programs need to be put in place in order to ensure organizations are able to counter cyberattacks.

Deposit-taking savings and credit cooperative societies may benefit from the findings of this study. This study recommends that staff education should be done regularly and training materials should be updated as new sophisticated malware arise. Human beings are considered to be the weakest link and in order for organizations to be fully prepared to prevent cyber-attacks they need to ensure employees understand risks and threats that some of their actions may pose and the best practices to follow in order to protect themselves online. In order to keep critical customer data safe users handling customer data, need to be trained on how to recognize and avoid common social engineering scams. This study further recommends that in order to be prepared for cyberattacks technical personnel need to be trained in order to equip them with the necessary skillset to deal with cybersecurity incidents. It is recommended to have an individual or individuals that are solely employed to deal with cybersecurity. Having one technical staff that deals with IT roles and cybersecurity roles may lead to the individual being overwhelmed with other tasks within the organization.

REFERENCES

[1] ACS (2016). Cybersecurity *Threats, challenges, Opportunities.* Retrieved from https://www.acs.org.au/ content/dam/acs/acspublications/ACS_Cybersecurity_Gui de.pdf.

[2] Aitel, D. (2012, July 18). *Why you shouldn't train employees for Security Awareness.* Retrievedfromhttps:// www.csoonline.com/article/2131941/why-you-shouldn't-train-employees-for-security-awareness.html.

[3] Aloul, F.A., (2012). The need for effective information security Awareness. *Journal of Advances in Information Technology, Vol 3*(3), 176-183

[4] Antwi-Bekoe. E. & Nimako. G.S., (2012) Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Institutions in Ghana. *Journal of Science and Technology Vol.1 No. 7, July 2012* pp 358 – 375.

[5] Bandura, A., (1986). Social foundations of thought and action: A social cognitive theory.

[6] Barton, K. A., Tejay, G., Lane, M., & Terrell, S., (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9–25.

[7] Beccaria, C. (1963) *On Crimes and Punishment*. Macmillan, New York.

[8] Bernik, I., & Prislan, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *PloS one*, *11*(9), e0163050. DOI:10.1371/journal.pone.0163050

[9] Bonnevier & Heimlen, (2018). *Role of firewalls in network security: A prestudy for firewall* threat *modeling*, (Masters dissertation, electrical engineering, and computer science, KTH Royal Institute of Technology).

[10] Borg, W.R, Gall, M.D., & Gall, P.J., (2007) *Educational Research*, 8th Edition

[11] Burke, D., (2018, Feb 6). *Large businesses lose an average of $1.05 million to cybercrime annually.* Retrievedfromhttps://www.globenewswire.com/newrelease/2018/02/06/1333676/0/en/Hiscox-Cyber-Readiness-Report-reveals-seven- out-of- ten-firms-fail-cybersecurity-readiness-test.html.

[12] Burns N. & Grove S. (1997) *The Practice of Nursing Research: Conduct, Critique and Utilization*. 3rd edition. WB Saunders Company, Philadelphia.

[13] Buss, M.D., & Salerno, L. (1984). Common sense and computer security. *Harvard business review*, *62 2*, 112-121.

[14] Carmines E.G & Zeller R.A., (1979). *Reliability and Validity Assessment*, Newbury Park, CA, SAGE.

[15] Carota, F.E, Granger M.M. & Douglas C. S. Cybersecurity incident response. Capabilities in the Ecuadorian financial sector, *Journal of Cybersecurity*, Volume 4, Issue 1, 1 January 2018, tyy002. https://doi.org/10.1093/cybsec/tyy002.

[16] Chenoweth, T., Minch, R., Gattiker, T. (2009). Application of protection motivation Theory to Adoption of Protective Technologies, *42nd Hawaii International Conference on System Sciences*, 1-10, doi: 10.1109/HICSS.2009.74.

[17] Compeau, D., Higgins, C., & Huff, S. (1999). Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study. *MIS Quarterly*, *23*(2), 145-158. doi:10.2307/249749.

[18] Cumby, B. (2006). The Value of Customer Relationships, *CA magazine*, p.7.

[19] Cybersecurity Ventures (2019). Cybercrime damages $6 trillion by 2021 Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[20] D'Arcy, J., Hovav, A. D. Gallett. (2008). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse. *Information Systems Research, Articles*, pp. 1–20

[21] Davis, M., & Borland, D. (2018). *U.S. Patent No. 9,876,735*. Washington, DC: U.S. Patent and Trademark Office.

[22] De Vaus, D. A. (2001) *Research Design in Social Research*. London: Sage.

[23] Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, *45*(1), 67–87

[24] Engeström, Y., Miettinen, R. Punamäki, R.L., (1999). Perspectives on Activity Theory. *Cambridge University Press*, *2*(10), 50.

[25] E&Y (2018) Is cybersecurity about more than protection. Retrieved from https://www.ey.com/Publication/ey-global-information-security- survey/201819/$FILE/ey-global-information-security-survey-2018-19.pdf.

[26] FAO (2018). *The current state of Agricultural Co-operatives in Kenya*. Retrieved from http://www.fao.org/3/x3138e/x3138e05.html.

[27] Grove (2018). Recent cyberattacks in South Africa. Retrieved from https://www.groveis.com/blog/grove-mitigate-cyber-attacks-in-south-africa- Mimecast-dark trace

[28] Hansche, S. D. (2002). Making Security Awareness Happen. In H. F. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (4th ed., *Vol*. 3, pp. 337-351). New York: Auerbach Publications.

[29] Herath. T., Rao, H. (2009), Protection Motivation and deterrence, A framework for security policy compliance in organizations. *European Journal for Information Systems*, *18*(2), 106-125.

[30] Herjavec Group (2019), *2019 Official Annual Cybercrime Report*. Retrieved from https://www.herjavecgroup. com/wp-content/uploads/2018/12/CV-HG-2019- OfficialAnnual-Cybercrime-Report.pdf

[31] Hiscox (2018). *Cyber Readiness Report* https://www.hiscox.com/cybersecurity

[32] Hong, K.S., Chi, Y.P., Chao, L.R., &Tang, J.H. (2003). An integrated system theory of information security management. Information Management & Computer Security, *Emerald journal*, *11*(5), 243–248.

[33] Huck, S. W. (2007). *Reading Statistics and Research.* United States of America, Allyn & Bacon.

[34] ITU (2018). *Global cybersecurity Index 2018* , Retrieved from https://www.itu.int/en/ITU- D/Cybersecurity/ Documents/draft-18-00706_Global-Cybersecurity-Index- EV5_print_2.pdf

[35] Jaatun, M. G., Johnsen, S. O., Bartnes, M., Longva, O. H., Tøndel, I. A., Albrechtsen, E., & Waero I., (2007), Incident Response Management in the oil and gas industry, Sintef.Retrieved from: https://brage.bibsys.no/ xmlui/bitstream/handle/11250/237 5186/Incident/Management

[36] Jasperson, J., Butler, B.S., Carte, T.A., Croes, H.P, Saunders, C.S., & Zheng, W.(2002). Review Power and Information technology research: A metal triangulation review. *MIS Quarterly*, *26*(4), 397-459

[37] Kankanhalli, A., Teo, H. H, Bernard C.Y. Tan & K.W. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139-154.

[38] Kapoor (2018, January 12). *How to tackle the cybersecurity skills gap in SA*. Retrieved from https://businesstech. co.za/news/it-services/219153/how-to-tackle-the- cybersecurity-skills-gap-in-sa/

[39] King, W.R., & Zmud, R. W. (2015). Managing Information Systems: Policy Planning, Strategic Planning, and Operational Planning. Paper presented at the *Proceedings from the 2nd International Conference on Information Systems*, Boston, MA.

[40] Knapp, K.J., Marshall, T.E., Rainer, R.K. and Morrow, D.W. (2006), The top information security issues facing organizations: what can government do to help, *Journal of Information Systems Security*, *15* (4), 51-58.

[41] Kothari, C.R. (2004). *Research Methodology Methods & Techniques.* (2nd ed.). New Delhi: New Age International publisher

[42] Kothari, C.R. (2010). *Research Methodology Methods & Techniques.* (3rd ed.). New Delhi: New Age International publisher

[43] Krejcie, R.V., & Morgan, D.W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement, 30,* 607-610

[44] Kuutti, K. (1995). Activity theory as a potential framework for human interaction research. *Journal of Information Systems Security*, *20* (4), 61-58.

[45] Laudon, K.C., & Laudon, J.P. (2019). Management Information Systems: Managing the Digital Firm

[46] LeCompte, M. D., & Preissle, J. (1993). *Ethnography and Qualitative Design in Educational Research* (2nd ed.). New York: Academic Press

[47] Lee S.M., Luthans, F. and Olson, D.L. (1982), A management science approach to contingency models in organizational structures. *Academy of management journal*, *25*(3), 553-66

[48] Lee, D., Larose, R., Rifon, N. (2008). Keeping our Network safe: a model of online protection behavior. *Behavior &InformationTechnology*,*27*(5), 445-454.

[49] Marczyk, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of behavioural science series. Essentials of research design and methodology.* Hoboken, NJ, US: John Wiley & Sons Inc.

[50] Milne, S., Sheeran, P. Orbell, S., (2000). Prediction and intervention in health-related behavior: A metanalysis review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1),106-143.

[51] Ministry of Industry Trade and cooperatives (2014). History and Organization of Cooperative. *Development and Marketing Sub Sector in Kenya*. Retrieved from http://www.industrialization.go.ke/index.php/downloads/123-history-and- organization-of-cooperative-development-and-marketing-sub-sector-in-kenya

[52] Mitnick, K. (2003). Are You the Weak Link? *Harvard Business Review*, *81*(4), 18-20.

[53] Mugenda, O. & Mugenda, A. (2003). *Research methods: quantitative and qualitative approaches*. Nairobi: Acts Press.

[54] Mugenda, A. G. (2008). *Social science research: theory and principles*. Nairobi: Acts Press.

[55] Musuva, K. P. (2015). *Kenya Cyber Security Report 2015: Achieving enterprise resilience through situational awareness*. Retrieved from https://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

[56] Mwitari (2018) Revealed: Why your savings in SACCOs are not safe, *Standard Digital*. Retrieved from:https:// www.standardmedia.co.ke/business/article/2001300957/revealed-why-yoursavings-in-saccos-are-not-safe

[57] Ndung'u M., Kandel, S. (2015). Information security management in organizations (Masters Dissertation, Centria University of Applied sciences).

[58] NIST (2019). Information security policy Retrieved from https://csrc.nist.gov/glossary/term/information-security-policy

[59] Orodho, C.R. (2009). Elements of Education and Social Science Research Methods.(2ndEdition). New Delhi: Kanezja PublishersPPOA. (2009).

[60] Oso, W. Y., & Onen, D. (2009). A general guide to writing research proposal and report. Nairobi: Jomo Kenyatta Foundation

[61] Ponemon Institute (2012). *State of SMB Cybersecurity Readiness: UK Study*. Retrieved from https://www. faronics.com/assets/UK-Faronics-FINAL-1.pdf

[62] Räikkönen, I.A (2017), *Motivations behind employee information security behavior* (Master's dissertation, Technical University of Finland, Finland) Retrieved from https://pdfs.semanticscholar.org/3761/901d554605de8b 122832e9de9a2f1d157731 .pdf

[63] Reid (2018). Cybersecurity Starts at the Top: Why Top Management Must Set the Tone for Data Security. Retrieved from: https://www.onserve.ca/cybersecurity-starts-at- the-top-why-top management-must-set-athe-tone-for-data-security/

[64] Richmond, C. (2017). Cybersecurity Readiness: How at risk is your organization

[65] Robinson, J. (2009). *Triandis theory of interpersonal behaviour in understanding software privacy behaviour in the South African context. (*Master's Dissertation, University of the Witwatersrand).

[66] Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change, *Journal of* Psychology, *91*(1), 93-114.

[67] Rogers, R. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A revised Theory of Protection Motivation. *In Social Physiology: A Sourcebook*, New York, 153-176

[68] Sanders, Lewis & Thornhill (2000). *Research methods for business students*. London: Pearson Education Ltd.

[69] Santillan, M. (2018) 75 Percent of Orgs Can't Effectively Detect and Respond to Data Breaches, Reveals Survey75 Percent of Orgs Can't Effectively Detect and Respond to Data Breaches, Reveals Survey. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/75-percent-orgs-can't-effectively-detect-respond-data-breaches-reveals-survey/

[70] SASRA (2018) The Sacco subsector 2018. Retrieved from https://www.sasra.go.ke/index.php/regulation/the Saccosubsector#.XH4K74gzbIU

[71] Sekaran, U. (2003). *Research Methods for Business. A Skill Building Approach*, 4th ed, NewYork: JohnWiley & Sons Inc.

[72] Serianu (2016). *Africa cybersecurity report Achieving Cyber Security Resilience: Enhancing Visibility and increasing awareness*. Retrieved from https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[73] Show J. (2007) Information security in practice from an Activity-Theoretic perspective. *Proceedings of the 6th Annual Security Conference*, Las Vegas, NV, 1-8.

[74] Signe, K. & Signe, L. (2018) *Cybersecurity in Africa: securing businesses with a local approach with global standards* Retrieved from https://www.brookings.edu/blog/africa-in-focus/2018/06/04/cybersecurity-in- Africa-securing-businesses-with-a-local-approach-with-global-standards/

[75] Simon, H. A. (1957). *Administrative Behavior* (2nd ed.). New York: The Free Press.

[76] Siponen, M. & Puhakainen, P. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757-778. 10.2307/25750704.

[77] South African Banking Risk Information Centre (2018). Digital Banking Crime Statistics. Retrieved from https://www.sabric.co.za/media-and-news/press-releases/digital- banking-crime-statistics/

[78] Straub, D., and Welke, R. (1998), Coping with Systems Risk: Security Planning Models for Management Decision Making, *Management Information Systems Quarterly*, 22(4), pp. 441-469.

[79] Sullivan, P. (2016). *Achieving cybersecurity readiness: what enterprises should know* Retrieved from https://searchsecurity.techtarget.com/tip/Achieving-cybersecurity- readiness-What-enterprises-should-know

[80] Tabachnick, B. G., & Fidell, L. S. (2007). Using Multivariate Statistics (5th ed.). New York: Allyn and Bacon

[81] Tanui (2018, December 18). SACCOs will experience double cybersecurity attacks in 2019. Retrieved from https://kenyanwallstreet.com/saccos-will-experience- double-cybersecurity-attacks-in-2019-serianu/

[82] Tashakkori, A. &Teddlie, C. (2003). *Handbook of Mixed Methods in Social & Behavioral Research.* Thousand Oaks: Sage.

[83] TESPOK (2016). *Cyberthreats an industry and sector's perspective Report*, Retrieved from https://www. tespok.co.ke/wp content/documents/TESPOKiCSIRT_ Cyber_ Security_ Report2016.pdf

[84] Trochim & William M.K. (2006). Research Methods Knowledge Base.

[85] Vygotsky, L. S. (1978). Mind in society: The development of higher psychological processes. *Harvard University Press*, *10*(5), 33

[86] Waweru, K.M. (2011) An investigation into the cash balance Management Approaches in SACCOs in Nakuru County *Journal of Business Studies Quarterly 2011, (2*(4), 17-26

[87] Wellington, J. (2000) Educational research: *Contemporary issues and practical approaches*. Continuum, London.

[88] Whitley, B. E. (2002). *Principals of Research and Behavioural Science*, Boston, McGraw-Hill.

[89] Whitman, M. E., Townsend A.M, Alberts.R.J., (2001). Information systems security andthe need for policy. *Information Security Management: Global Challenges in the New Millennium*. Idea Group Publishing, Hershey, PA, 9–18.