FACTORS INFLUENCING CYBERSECURITY READINESS IN DEPOSIT TAKING SAVINGS AND CREDIT COOPERATIVES: A CASE STUDY OF NAIROBI COUNTY

Nancy Nyawira Muraguri
Master of Information and Communication Technology Management, Jomo Kenyatta University of Agriculture and Technology, Kenya

Dr. Tobias Mwalili
Jomo Kenyatta University of Agriculture and Technology, Kenya

Dr. Thomas Mose
Jomo Kenyatta University of Agriculture and Technology, Kenya

International Academic Journal of Information Systems and Technology (IAJIST) | ISSN 2518-2390

Received: 20th September 2019
Accepted: 18th October 2019

Full Length Research

Available Online at:

http://www.iajournals.org/articles/iajist_v2_i1_157_182.pdf

Citation: Muraguri, N. N., Mwalili, T. & Mose, T. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County. *International Academic Journal of Information Systems and Technology, 2*(1), 157-182

ABSTRACT

Savings and credit cooperative societies in Kenya are riddled with cyber-attacks. Despite the warning on the increase in cyberattacks most of these SACCOs are not cyber ready this, therefore, raises doubts on their ability to keep customer data safe. The purpose of carrying out this study was to establish the factors that influence SACCO's ability to detect, prevent and respond to threats. The aim of this study was to determine how factors such as staff training and awareness on cybersecurity, cybersecurity policies, top management support, and technical and logical controls influence cybersecurity readiness of deposit-taking SACCOs. 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 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. The findings of the study revealed that there is a positive and significant correlation between staff training, top management support, technical and logical controls 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. It was also concluded that an organization with efficient and updated cybersecurity policies are ready to handle all cybersecurity issues including preventing them from occurring and that top management needs to prioritize and enact policies that will protect the organization's assets and they need to embody cybersecurity into their long-term strategy. The study recommended that more training programs are organized regularly; cybersecurity policies should be reviewed and updated regularly, and top management support and technical and logical controls should be maintained alongside other factors to enhance cybersecurity readiness.

Key words: *cybersecurity readiness, deposit taking, savings and credit cooperatives, Nairobi County*

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.

Most African countries have become totally dependent on ICT. Governments have introduced e-government in order to improve service delivery to its citizens. Africa has recorded a very high rate of cybercrime with a total cybercrime cost of 895 million US dollars in 2016 and financial institutions are most affected by cybercrime (Serianu, 2016). Serianu (2017) surveyed banks and financial institutions from ten African countries and found out that these financial institutions lost a combined total of 248 million US dollars with governments losing 204 million US dollars.

The highest threats for financial institutions came from banking malware, insider threats, and Automated Teller Machine (ATM) skimming. Majority of organizations in Africa are not prepared to address cybersecurity threats this is due to the lack of skilled professionals, inadequate budgets and the lack of visibility within the organization. Countries such as South Africa saw an increase in cybercrime. According to the South African Banking Risk Information Centre (2018), South Africa loses 152.6 million US dollars a year to cyber attacks this; therefore, makes South Africa have the third-highest number of cybercrime victims worldwide.

Africa as a whole has a shortage of experienced and qualified professionals with the relevant skill required to support cybersecurity in organizations. Specialists in cybersecurity choose to be mobile and most of them opt to move to first world countries (Signe & Signe, 2018). African organizations, therefore, need to invest heavily on developing skills of its technical personnel involved in cybersecurity; they should also come up with strategies on how they can retain top talent.

Over the past decade, Kenya has experienced tremendous growth in the use of Information Communication Technologies (ICT). The growth of systems such as Mpesa which is widely used as an alternative to transact has made money transfer quicker, cheaper and reliable over greater distances. Kenya has been at the forefront of establishing the necessary cybersecurity governance framework for the country, recently the country introduced the Computer Misuse and Cybercrimes Act, 2018 which is expected to restrain cybercrimes and any other computer-related crimes. The law enables timely detection, prohibition, response, and investigation of cybercrime. Despite having the necessary cybersecurity laws in place computer-related offenses are still soaring. According to Serianu (2017), the estimated cost of cybercrime in Kenya soared to 210 million US dollars in 2017. Systems such as mobile money in Kenya have experienced various attacks through social engineering, account personifications and use of malware.

Adversaries are now exploiting the weak security controls around the mobile money platform to steal from unsuspecting subscribers. The National ICT policy (2016) highlights the strategies on how to improve cybersecurity in the country; however, challenges such as lack of skills, lack of information security awareness and a culture that fosters the adoption of internet security hinder effective cybersecurity readiness of organizations within the country. Most organizations don't budget for training and awareness of their staff. The lack of employee training and awareness has increased the organization's vulnerability to attacks.

According to ITU (2018) Kenya ranks second in Africa in the global cybersecurity index, Kenya has set a good example of cooperation and collaboration through the establishment of National Kenya Computer Incident Response Team Coordination Centre (National KECIRT/CC). The CIRT in Kenya collaborates with ISPs, education institutions and financial institutions. Regionally it works with other CIRTs through the East African Communications institutions, and internationally the CIRT liaises with organizations such as ITU and other countries such as the United States and Japan and others. According to TESPOK (2016), the most attacked sector in

Kenya is the telecommunications industry due to misconfigurations of the security technologies and the network this leads to denial of service to providers. The country has also experienced an increase in the amount of malicious mobile applications that circulate in legitimate third-party sites and app stores. The government through the Communications Authority of Kenya (CAK) has been keen on the dissemination of security advisories immediately vulnerabilities are announced; this has acted as a preventative measure for organizations within the country towards cyber-attacks.

Most organizations in Kenya are unprepared and not fully equipped to respond and deal with the number of evolving sophisticated cybersecurity threats (Serianu, 2016). Even though regulators such as Central Bank of Kenya (CBK) and Insurance regulatory authority (IRA) have provided guidelines to address information security issues, these initiatives cannot be enough to dissuade cybercrime, organizations need to ensure that they train their employees and also need to institute practices needed to protect their critical infrastructure.

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 factors that influence cybersecurity readiness in deposit-taking SACCOs.

GENERAL OBJECTIVE

The general objective of the study was to determine factors influencing cybersecurity readiness in deposit-taking SACCOs.

SPECIFIC OBJECTIVES

1. To determine the influence of staff training and awareness on cybersecurity readiness in deposit-taking SACCOs
2. To determine the influence of cybersecurity policies on cybersecurity readiness in deposit-taking SACCOs
3. To determine the influence of top management support on cybersecurity readiness in deposit-taking SACCOs
4. To determine the influence of technical and logical security controls on cybersecurity readiness in deposit-taking SACCOs

THEORETICAL FRAMEWORK

A theoretical framework is a collection of interrelated concepts that can be used to direct research with the purpose of predicting and explaining the results of the research (LeCompte & Preissle, 1993). Theoretical frameworks have a predictive value, which helps the researcher to make logical predictions and thus ask relevant research questions. In addition to their explanatory power, theoretical frameworks have predictive value, which helps researchers to make logical predictions and thus ask appropriate research questions (Wellington, 2000).

Activity Theory

The activity theory was pioneered by Lev Vygotsky, Sergei Rubinstein, and Alexei Leont'ev. According to Vygotsky (1978), human beings do not act directly with the environment but by means of mediating factors such as environment, culture, history of a person, motivations, artifacts, and complexity of real-life activities. Engstrom (1987) contributed to this theory and proposed that activity consists of components including subjects, objects, and the community, tools (the artifacts), rules and the division of labor. The main goal of human activity is to produce certain artifacts in order to transform it into certain outcomes. In order to achieve an outcome, subjects share tools with a division of labor in order to achieve an objective. The activities are arbitrated with the rules and regulations of the community and environment that draws the limits in which the activities should be performed (Kuutti, 1995). Show (2007) applied the activity theory to the context of information security by examining the contextual and systemic contradictions that non-technical staff experience. The impact of social and cultural factors on occurrences of security breaches, which are as a result of non-compliance and normalized carelessness with policies and procedures, may be revealed as symptomatic of tensions and systemic contradictions. Applying this theory to our study security factors such as policies influence how employees respond to cybersecurity threats such as how non-technical staff manages customer records and confidential information, also how they respond to social engineering scams and phishing emails.

Protection Motivation Theory

Rogers (1975) proposed the protection motivation theory in order to understand fear appeals and how people cope with them. The theory suggests that the perceived severity of a threat, the probability of the occurrence of a threat, and the effectiveness of a protective response can cause a cognitive mediation process in an individual who is motivated to protect themselves from the potential threat (Chenoweth *et al*., 2009). According to the theory, there are two cognitive processes encouraging people to participate in actual protection behavior; threat appraisal and coping appraisal (Rogers, 1983). The threat appraisal consists of perceived severity and perceived vulnerability of a situation. Perceived vulnerability is the subjective perception an individual believes the possibility of a threatening incident happening to him or her. Hence, the likelihood of adopting the necessary protection increases when a person perceives he or she will experience higher vulnerability (Lee, 2008). Perceived severity refers to the magnitude of the consequences of an incident if the threat succeeds (Milne *et al*., 2000). The consequences may include damage to the organization's reputation, identity theft, compromise and leakage of customers' data and financial records. The more an individual perceives the threat can significantly damage them, and their organization and their customers, the individual is more likely to be concerned about information security (Herath & Rao, 2009).

A coping appraisal consists of response costs, self-efficacy response efficacy. Self-efficacy refers to a belief in one's ability to perform a recommended task. When an individual believes she or he has the skills to perform a specific task, the individual will take the necessary action (Lee *et al*., 2008). Using the protection motivation theory, the authors suggested that self-efficacy can be a predictor of behaving with the intention to implement virus protection in order to improve information security. Chenoweth *et al*., (2009) described response efficacy as the belief that the recommended response will be effective in reducing the risk. Whilst response cost affiliated with various types of costs entailed in the recommended behavior (for example time, cognitive effort). Applying this theory to our study, organizations need to educate employees on the information security risks and dangers of using weak passwords and giving out customer data is an effective way to reduce cyber-attacks and prevent data loss. Professional training of technical staff on how to prevent, anticipate, respond and set up technical controls minimizes risk to cyber-attacks within the organization.

Social Cognitive Theory

Social Cognitive Theory (SCT) is mainly used in education and psychology, this theory proposes that parts of an individual's knowledge acquisition can be directly correlated to observing others. Bandura (1986) further advanced this theory as an extension of his social learning theory. This theory revolves around the process of learning directly or acquiring knowledge correlated to the observation models such as media sources, an individual has the freedom to choose the environment in which they exist in addition to being affected by the environment (Compeau &

Higgins, 1995). Moreover, both behaviors in a given situation and the environment influence each other. Finally, the behavior is affected by cognitive and personal traits. Bandura (1986) introduced self-efficacy as a major cognitive force guiding individual behavior. He defined self-efficacy is a person's judgment of their capabilities to perform a task. Self-efficacy beliefs act as a crucial set of proximal determinants of human motivation and action. The context of Information Technology (IT), the research suggests that individuals who possess high self-efficacy toward IT use IT more frequently (Compeau, Higgins, & Huff, 1999). This theory is relevant to our study since it elaborates how a judgment of one's ability to tackle a problem such as how to respond to fraudsters requesting for customer's information and not opening emails from unknown senders influences cybersecurity within their organization.

Integrated Systems Theory

Hong *et al*., (2003) proposed the integrated systems theory. This theory incorporates cybersecurity policy, contingency management, risk management, information auditing, and internal control theories. The contingency management entails managing the interaction between environmental variables such as security threats and managerial variables to achieve organizational objectives (Lee *et al*., 1982). This theory incorporates a sequential process which originates from security policy theory, risk management, internal control (which includes personnel security control, systems and network security control and business continuity management) and information auditing. This theory views cybersecurity as a function of all those components. Applying this theory to our study organizations need to have the necessary security controls in their environment and being able to manage risks that arise from vulnerabilities that occur from poor configurations and poor security controls. This theory also highlights the importance of top management being involved in formulating cybersecurity policies, establishing security strategies and fostering a security culture within the organization.

EMPIRICAL REVIEW

Staff training and awareness on cybersecurity

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.

Cybersecurity Policies

NIST (2019) defines a cybersecurity policy as a collection of regulations, directives, rules and best practices that give guidance on how organizations should protect their critical infrastructure and critical data. Policies offer procedural instructions for employees and workers to follow should an incident arise. Ndung'u and Kandel (2015) argued that the policies must be well communicated to all concerned personnel. The researchers found out that having a security policy was crucial since it fully engages employees to participate in safeguarding the organization's data and decreases the risk of a security breach caused by the human factor. Kamariza (2017) noted that the lack of cybersecurity policy in an organization puts the organization at high risk. This implies that the organization has a less understanding of its most sensitive data and information. This also implies that the organization does not have a strong awareness regarding possible vulnerabilities and how to respond in the event of a cyberattack on the organization.

Raikonen (2017) deduced that clearly documented policies and proper communication of these policies are important to employees committing to adhering to cybersecurity policies and

procedures in order to ensure that the organization's assets are safe. He also noted that the lack of knowledge on cybersecurity policies affected employee's compliance with cybersecurity policies hence putting the organization at risk. Cybersecurity policy has been called the precondition to implement all effective security deterrents Straub (1990) and may be more vital to reducing computer crime than devices like firewalls and intrusion detection systems (Buss & Salerno, 1984).

Antwi-Bekoe and Nimako (2012) suggested that it is important for the management in an organization to obtain feedback on user awareness on cybersecurity best practices in order to develop strategies towards ensuring the effectiveness of the policy. They suggested that any organization that has a cybersecurity policy regarding the securing the organization's systems and data should occasionally get feedback on how well the end-users of the systems are aware of the issues likely to compromise the organization computer systems and how well they adhere to the policy.

Top Management Support

The Ponemon Institute (2012) conducted a study on the state of small business's cybersecurity readiness in the United Kingdom. The study found out that one of the barriers for organization's cybersecurity readiness was the lack of monitoring of end-users; it is the role of senior management to monitor users and ensure those cybersecurity policies are adhered to. Jasperson *et al*., (2002) conducted a meta-analysis postulated about top management support. The authors postulated that top management's failure to exercise formal authority especially on information security policies leads to an influencing behavior by subordinates. Dutta and McCrohan (2002) stated that effective organizational cybersecurity does not start with antivirus software or firewalls, but with top management. Knapp *et al*., (2006) suggested top management plays an important role in cybersecurity readiness by supporting employees training, promoting a security-aware culture, and insisting on the compliance of security policies by staff. Kankanhalli *et al*., (2008) suggested that organizations with top management support were found to engage in more preventive efforts than organizations with weaker support from top management. This support leads to the success of information effectiveness and a reduction in the cybersecurity risk.

Antwi-Bekoe and Nimako, (2012) conducted a research on computer security awareness and vulnerabilities; they found out that low awareness levels of management regarding the security risks involved resulted in a higher vulnerability of the organization. Barton *et al.,* (2016) deduced that top management commitment alone does not assure effective risk management, however it is crucial for the implementation of security technologies, enforcement, and compliance with cybersecurity policies within the organization. Catota *et al*., (2018) found out that the barriers that Ecuadorian financial institutions face that prevent them from properly respond to security incidences were low budget; the low budget affects the number of security controls that were implemented within the organizations. They suggested that executive managers need to be

educated about the importance of protecting the organization's data and they need to be convinced to invest in security technologies in order to improve threat detection. Therefore, the study sought to assess how top management support impacts cybersecurity readiness in SACCOs.

Technical and Logical Security Controls

Ponemon Institute (2012) conducted a study on the state of small business's cybersecurity readiness in the United Kingdom. The study found out that one of the barriers for an organization's cybersecurity readiness was insufficient technology resources. Organizations that lacked the necessary technologies had experienced more cyber-attacks. Catota *et al.*, (2018) conducted a research on the cybersecurity incident response capabilities in the Ecuadorian financial sector and found out that one of the barriers that Ecuadorian financial institutions face that prevents them from properly responding to security was inadequate security controls and lack of technologies.

Bernik and Prislan, (2016) conducted a study with the aim of measuring information security performance within organizations. The authors found out that technical and logical control were key success element to ensuring that an organization has the right security posture thereby being prepared to prevent, detect and respond to threats. The researchers went further and recommended that cybersecurity needs to evolve systematically and that the beginning steps should include technical, logical security controls to ensure that organizations are able to effectively respond to security incidences.

Bonnevier and Heimlen, (2018) conducted a study on the role of firewalls in network security and found out that most firewalls configurations did not match the organization's security policies and some organizations did not have any configurations set on the firewalls. Most firewalls lack configurations due to the poor understanding of the organization's policies or lack of organizational policies for firewalls. Generally, if a firewall allows an unauthorized agent to access internal systems or information, it should most likely be considered to lead to information security risk because malicious networks are accessed by the user and are undetected by the firewall.

RESEARCH METHODOLOGY

Research Design

A research design is an overall strategy for conducting the research. A research design integrates the different components of the study in a logical and cohesive manner; it constitutes the layout for the collection, measurement, and analysis of data (DeVaus, 2001). This study adopted a descriptive research design. According to Kothari (2004), a descriptive research study is one that is concerned with describing the characteristics of an individual or a group. This study used a descriptive research design since it allows for an in-depth study of the subject matter in a quantitative aspect of the overall research. This design enabled the researcher to gain the

information required since the intention of the study was to assess, understand and gain knowledge and insight on the factors that influence cybersecurity readiness in deposit-taking SACCOs.

Target Population

The target population is the entire accumulation of respondents that meet the designated set of criteria and from which the study population is drawn from (Tabachnick & Fidel, 2013). According to SASRA (2018), there are 40 licensed deposit-taking SACCOs in Nairobi County; therefore, the target population consisted of a census of all the 40 licensed deposit-taking SACCOs in Nairobi County. The respondents of this research proposal were employees from all the 40 deposit-taking SACCOs. The respondents of this study comprised of 1 ICT department staff, 1 top manager and 1 customer service department staff. The population targeted was the employees responsible for the implementation of cybersecurity policies, provision of technical support and responding to incidences and interacting with customer data. The total study population was 120. The respondents were selected randomly.

Sample Frame

A sampling frame is a list, index or a directory of cases from which a sample can be selected. Subjects selected from the sampling frame form the units of observation (Mugenda & Mugenda, 2010). A sample size of more than 10% is a relatively good representation for the descriptive survey in a relatively big population (Mugenda & Mugenda, 2003). The sampling frame for the study was 40 deposit-taking SACCOs in Nairobi County.

Sampling Technique and Sample Size

Borg and Gall (2007) define a sample as a subgroup carefully selected so as to be a representative of the whole population with the relevant characteristic. The authors also define sampling as the process of selecting a number of individuals in such a way that they represent the large group from which they were selected. For this research, a census was conducted in all the nine sub-counties where all the SACCOs in each sub-county participated. A census enables a complete enumeration of all items in the population (Oso & Onen, 2009).

Data Collection Instruments

The main data collection instrument that was used in this study was the questionnaire. This study used both primary and secondary data. Questionnaires were used for collecting primary data. Primary data was, therefore, collected directly from first-hand experience (Davis, 2018). Questionnaires provide an efficient way of collecting responses from a large sample prior to quantitative analysis (Saunders *et al*., 2000). The questionnaire was divided into seven main sections of investigation. The first section captured the demographic characteristics of the respondents. The next six sections focused on information relating to the key objectives of the study which included: staff training and awareness, cybersecurity policies, top management

support, and technical and logical security controls and how they influence cybersecurity readiness of deposit-taking SACCOs. The questionnaire was self-administered. The questionnaires had close-ended items and open-ended items. Responses to closed-ended questions were elicited on a 5-point Likert scale with 1 signifying strongly disagree, 2-disagree, 3 undecided, 4–agree and 5-strongly agree. Secondary data came from SASRA's Reports and publications and referred journals.

Data Collection Procedure

Prior to the commencement of data collection, the researcher obtained all the necessary documents, including an introduction letter to the SACCOs. The researcher explained the purpose of the study to the audience. Upon getting clearance, the researcher distributed the questionnaire in person to the respondents which was required to be filled within the agreed schedule. Use of questionnaires was expected to ease the process of data collection as all the selected respondents are reached in time. During the distribution of the instruments, the purpose of the research was explained by the researcher.

Data Analysis and presentation

Data analysis was conducted according to the research objectives. Before processing the responses, data preparation was done on the completed questionnaires. This involved screening and cleaning the data. Data was also edited to check for outliers and to clear out any data points that may hinder the accuracy of the results. Lastly, data was coded to enable responses to be grouped into categories. Data collected was analyzed by both descriptive and inferential statistics. Descriptive analysis methods such as measures of central tendency like mean and measures of dispersion such as standard deviation, as well as percentages were used in this study. Data analysis also used SPSS to generate quantitative reports which was presented in the form of a table, pie charts, and bar graphs. The researcher used multiple regression analysis to establish the relationship between the independent and dependent variables. 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 researcher used the following multiple regression analysis model. The model below was used to determine how cybersecurity readiness in SACCOs is influenced by the identified factors.

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon}$$

Where: Y= Cybersecurity readiness; β_0 = Constant; β_1, β_2, β_3, β_4 = Regression coefficients; X_1= Staff training and awareness; X_2 = Cybersecurity policies; X_3= Top management support; X_4= Technical and logical security controls; ε = Error term

RESEARCH RESULTS

The general objective of this study was to determine the factors influencing cybersecurity readiness in deposit taking SACCOs, the study focused on deposit taking SACCOs within

Nairobi county. This study sought to examine the factors that influence cybersecurity readiness in deposit-taking SACCOs. The four specific objectives for the study were to determine the influence of staff training and awareness, cybersecurity policies, top management support and technical and logical security controls on cybersecurity readiness in deposit-taking SACCOs.

Staff Training and Awareness

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 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.

Cybersecurity Policies

The results of the study indicated that the majority of the SACCOs have a formulated ICT security policy in place. It was also found that the ICT policy was not available and accessible to the majority of the respondents. This is perhaps because the issues of ICT security are solely handled by the ICT department, who are allowed access to information security. The employees who access the cybersecurity policy do so through a shared folder or the intranet. In most SACCOs, the cybersecurity policy is regularly reviewed and updated. However, most of the respondents indicated that they are not regularly trained and there is no proper communication whenever changes are made to the cybersecurity policy. It was also evident that the current policy is fully implemented. The results of regression and correlation analysis revealed that there is a positive and significant correlation between cybersecurity policies and cybersecurity readiness. This implies an improvement in cybersecurity policies leads to improved cybersecurity readiness.

Top Management Support

The results indicated that most of the top management in various SACCOs allocate ICT budget of 35% and below. The majority of the respondents indicated that the top management is actively involved in security awareness sessions within the SACCOs. However, the results revealed that in most SACCOs, discussions involving cybersecurity are not considered a top priority and are not discussed in management meetings. This can be attributed management's perception of cybersecurity as a technical issue, therefore there needs to be more cybersecurity awareness among top managers. It was further revealed that SACCOs did not have personnel solely employed to managed cybersecurity, it was either the systems administrator or the ICT officer's job to deal with cybersecurity. In some SACCOs, the senior management is actively involved in monitoring cybersecurity progress, but this is not the case in the majority of the SACCOs. Besides, most SACCOs include cybersecurity in their long-term strategy. The correlation and regression results revealed that there is a significant positive correlation between top management support and cybersecurity readiness. This implies that an increase in top management support leads to a significant increase in cybersecurity readiness.

Technical and Logical Security Controls

The results of the study indicated that the majority of the SACCOs occasionally review the configurations on the security technologies. Most of the organizations do not have cybersecurity policies for the security technologies that have been implemented within the organization. It was also revealed that in most SACCOs, the ICT personnel are not capable of configuring the security technologies to prevent and detect threats. Most of the security technologies settings are left on default. This can be attributed to the fact that most SACCOs do not have well qualified staff solely employed to handle cybersecurity issues. The majority of the respondents agreed that the permissions to their organization's systems such as ERP and the core banking system are restricted to their core responsibilities such that they cannot perform incompatible functions or functions beyond their responsibilities. The correlation and regression results revealed that there is a significant positive correlation between technical and logical security controls and cybersecurity readiness. This implies that an increase in top management support leads to a significant increase in cybersecurity readiness.

Cybersecurity Readiness

The study established that the four objectives positively affected cybersecurity readiness of deposit taking SACCOs. The findings indicated that, by putting into consideration the four factors all indicators associated with cybersecurity readiness that is detection, response and prevention will be boosted and this is a sentiment shared by some of the respondents. Majority of the respondents indicated that their organizations were adequately prepared to detect, repond and mitigate cyberattacks. However, it is important to note that there are other factors (38.9%) not studied in this study that contribute to the cybersecurity readiness in SACCOs. Such factors may include organizational culture among others.

INFERENTIAL STATISTICS

The study used Pearson's product-moment correlation analysis and multiple regressions to assess the relationship between dependent and the independent variables. The data on cybersecurity readiness, staff training and awareness, cybersecurity policies, top management support and technical and logical security controls were computed into single variables per every factor. The Pearson's correlations analysis was done at a 95% confidence interval and a 5% confidence level 2-tailed. The correlation matrix is presented in table 1.

Table 1: Correlation Analysis

		CSR	ST	CSP	TMS	TLC
CSR	Pearson Correlation	1				
	Sig. (2-tailed)					
	N	100				
ST	Pearson Correlation	.279**	1			
	Sig. (2-tailed)	.005				
	N	100	100			
CSP	Pearson Correlation	.226*	.490**	1		
	Sig. (2-tailed)	.024	.000			
	N	100	100	100		
TMS	Pearson Correlation	.026**	.074	.318**	1	
	Sig. (2-tailed)	.006	.464	.001		
	N	100	100	100	100	
TLC	Pearson Correlation	.134	-.076	.112	-.020	1
	Sig. (2-tailed)	.003	.451	.267	.843	
	N	100	100	100	100	100

CSR=Cybersecurity Readiness; ST=Staff Training; CSP= Cybersecurity Policies; TMS= Top Management Support; and TLC= Technical and Logical security controls

The findings revealed that there is a positive significant correlation between staff training and cybersecurity readiness of magnitude 0.279, a positive significant correlation between cybersecurity policies and cybersecurity readiness of magnitude 0.226, a significant positive correlation between top management support and cybersecurity readiness of magnitude 0.026. The findings also revealed that there exists a positive and significant correlation between technical and logical security controls and cybersecurity readiness of magnitude 0.134.

Staff training, top management support and technical and logical security controls, and cybersecurity policies showed a significant P-value ($p<0.05$) at 95% confidence level. The significant values for the relationship between cybersecurity readiness, staff training and awareness, cybersecurity policies, and technical and logical security controls were 0.005, 0.024, 0.006, and 0.003 respectively. This implies that technical and logical security controls was the

most significant factor, followed by staff training and awareness, then followed by top management support, and finally cybersecurity policies.

Table 2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.781[a]	.611	.576	2.69472

The result presented in the model summary revealed that the independent variables in this study (cybersecurity readiness, staff training and awarenes, cybersecurity policies, top management support and technical and logical security controls) explain 61.1% of the cybersecurity readiness as represented by the R squared. This implies that there are other factors (38.9%) not studied in this study that contributes to the cybersecurity readiness in SACCOs. Such factors may include organization security culture among others.

Table 3: Analysis of Variance

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	83.918	4	20.980	2.889	.026[b]
	Residual	689.842	95	7.261		
	Total	773.760	99			

The significance value for the model is (P=0.026) which is less than 0.05 hence, the model is statistically significant in predicting how staff training and awareness, cybersecurity policies, top management support and technical and logical security controls influence cybersecurity readiness. The F critical at 5% level of significance and 95% confidence is 2.31. Since F calculated is greater than the F critical value = 2.889, this implies that the overall model was significant.

Table 4: Coefficient of determination

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.832	1.808		1.567	.121
	ST	.226	.105	.243	2.146	.004
	CSP	.124	.149	.099	.834	.007
	TMS	.014	.057	.026	.255	.029
	TLC	.210	.145	.142	1.441	.003

The outcome of the regression analysis presented in Table 4.18 produced a model equation as follows:

$$\mathbf{Y = 2.832 + 0.226\ X_1 + 0.124\ X_2 + 0.014\ X_3 + 0.210\ X_4 + \varepsilon}$$

Cybersecurity Readiness = 2.832+ 0.226 Staff training & awareness + 0.124 Cybersecurity Policies + 0.014 Top management support + 0.210 Technical & logical security controls + ε

The first 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 be an increased level of cybersecurity preparedness. The results of the regression equation revealed that a unity increase in staff training and awareness lead to a **0.226** on cybersecurity readiness. The findings supports previous studies. ACS (2018), that 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.

The second objective of the study was to determine the influence of cybersecurity policies on cybersecurity readiness in deposit-taking SACCOs. The regression results revealed that there is a significant positive correlation between cybersecurity policies and cybersecurity readiness at **β= 0.124; t = 0.834;** and **p = 0.007**. Therefore, cybersecurity policies positively influences cybersecurity readiness, hence an increase in cybersecurity policies leads to increased cybersecurity readiness. The results of the regression equation revealed that a unity increase in cybersecurity policies lead to a **0.124** increase on cybersecurity readiness. The results show the importance of having a well-communicated policy on cybersecurity, which is in support of findings by Ndung'u and Kandel (2015) who found that having a security policy was crucial since it fully engages employees to participate in safeguarding the organization's data and decreases the risk of a security breach caused by the human factor. They further noted that the policies must be well communicated to all concerned personnel.

The third objective of the study was to determine the influence of top management support on cybersecurity readiness in deposit-taking SACCOs. The regression results revealed that there is a significant positive correlation between top management support and cybersecurity readiness at **β= 0.014; t = 0.255**; and **p = 0.029**. Therefore, top management support positively influences cybersecurity readiness, hence, an increase in top management support leads to increased cybersecurity readiness. The results of the regression equation revealed that a unity increase in top management support leads to a **0.014** increase on cybersecurity readiness. The results are in support to a previous study by Knapp *et al*., (2006) who noted that top management plays an important role in cybersecurity readiness by supporting employees training, promoting a security-aware culture, and insisting on the compliance of security policies by staff.

The fourth objective of the study was to determine the influence of technical and logical security controls and cybersecurity readiness in deposit-taking SACCOs. The regression results revealed

that there is a significant positive correlation between technical and logical security controls and cybersecurity readiness at **β= 0.210; t =1.441;** and **p = 0.003.** Therefore, technical and logical security controls positively influence cybersecurity readiness, hence, an increase in the number of technical and logical security controls leads to increased cybersecurity readiness. The results of the regression equation revealed that a unity increase in cybersecurity policies lead to a **0.210** increase on cybersecurity readiness. These findings support a previous study by Bernik and Prislan, (2016) who found out that technical and logical control were key success element to ensuring that an organization has the right security posture thereby being prepared to prevent, detect and respond to threats.

CONCLUSIONS

Based on the findings of this study the research concluded staff training and awareness, cybersecurity policies, top management support and technical and logical controls influence cybersecurity readiness in deposit taking SACCOs. All the four variables have a positive impact on cybersecurity readiness in deposit taking SACCOs. Staff training was found to be the 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 servers will be inaccessible. Effective training programs need to be put in place in order to ensure organizations are able to counter cyberattacks.

The study also found that cybersecurity policies is also significant factor that positively influences cybersecurity readiness in deposit-taking savings and credit cooperative societies. Although most of the organization had a cybersecurity policy in place most of the non-technical staff were not able to access it. The study, therefore, concluded that an organization with efficient and updated cybersecurity policies that are accessible and any change made are effectively communicated to employees are ready to handle all cybersecurity issues is adequately prepared to handle cybersecurity incidents.

The study revealed that top management in most organizations are actively involved in security awareness sessions within the SACCOs but in their meetings, they do not give the issues of cybersecurity top priority since they consider cybersecurity to be a technical issue. The study concluded that top management support is a key pillar for cybersecurity readiness.

The study also found that technical and logical security controls have significant positive influence cybersecurity readiness. Most of the respondents were of the opinion that access controls have greatly contributed to a reduction of cybersecurity incidences especially when combined with the right technical controls. This study therefore concluded that technical and logical controls are important factors that positively influence cybersecurity readiness.

RECOMMENDATIONS

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.

The study recommends that the cybersecurity policy should be made available and accessible to all employees. This study also recommends that employees should be regularly taken through and trained on the cybersecurity policies and they need to be made aware of the possible vulnerabilities and how to respond in the event of a cyberattack in the organization. Disseminating proper knowledge of the cybersecurity policy to staff will ensure a high rate of compliance to the policies. In order to deal with new and sophisticated malware it is recommended that cybersecurity policies should be reviewed and updated regularly. Any updates made should be properly communicated to employees in order to ensure employees commitment to adhering to cybersecurity policies and procedures.

Top management needs to be actively involved in cybersecurity issues. A cyberattack may have a direct and indirect effect on the organization’s growth. Top management needs to be sensitized on the various losses the organization may incur in the event of a cyberattack. Such losses may include brand reputation, loss of customer trust, financial loss in the event of ATM jackpotting in organizations that have ATMs. They should also be educated on the importance of investing in proper security technologies that aim to improve threat detection. Active participation of top management on security issues sets in motion the proper security culture for the organization. They therefore need to support every security programme within the organization and insist on compliance of security policies.

Deposit taking SACCOs should heavily invest in various technical and logical controls in order to ensure critical systems are well protected. Security should not be seen as a one size fits all and organizations should focus on investing in various security technologies to deal with different variants of malware that use different attack vectors. A firewall can not prevent leakage of customer information by employees, however data loss prevention systems can prevent leakage of customer information. Professional training of technical personnel should be done regularly.

Most security technologies have complicated administration portals, staff that are in charge of security need to be trained on every bit of the administration of thee portals, how to configure certain policies such as blocking of devices or blocking sites. Most of the technical staff in these organizations do not have adequate knowledge on cybersecurity therefore these organizations should have an employee that is solely hired to handle cybersecurity issues. In order to have proper configurations on security technologies it is crucial to have specific policies for various security technologies that have been implemented within the organization. Such policies may include blocking of specific sites or blocking, these policies will therefore give technical personnel a roadmap on the configurations that need to be put in place on various security technologies.

As the SACCOs regulator SASRA should also be actively involved in ensuring customer data is protected. SASRA should come up with a framework on how SACCOs can implement training programs and they should also make it mandatory for SACCOs to report cyberattacks to the regulator in order to improve collaboration. This will in turn encourage intelligence sharing which can help strengthen resilience and reactivity to sophisticated threats within the sector.

Finally, the study recommends that SACCOs should regularly conduct vulnerability assessments and penetration tests in order to recognize major weakness in the organization's systems, ascertain how to allocate resources and enhance the security of applications and the organization's network as a whole.

REFERENCES

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

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.

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

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.

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

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.

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

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

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).

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

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.

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

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

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

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.

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.

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.

Cumby, B. (2006). The Value of Customer Relationships, *CA magazine*, p.7. Cybersecurity Ventures (2019). Cybercrime damages $6 trillion by 2021 Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

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

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

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

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

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

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.

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

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

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.

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.

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

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

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.

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

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

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.Retrievedfrom:https://brage.bibsys.no/xmlui/bitstream/handle/11250/2375186/Incident/Management

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

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.

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/

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.

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.

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

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

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

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

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

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

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

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

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.

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.

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

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

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

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

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

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

Ndung'u M., Kandel, S. (2015). Information security management in organizations (Masters Dissertation, Centria University of Applied sciences). NIST (2019). Information security policy Retrieved from: https://csrc.nist.gov/glossary/term/information-security-policy

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

Oso, W. Y., & Onen, D. (2009). A general guide to writing research proposal and report. Nairobi: Jomo Kenyatta Foundation Ponemon Institute (2012). *State of SMB Cybersecurity Readiness: UK Study*. Retrieved from: https://www.faronics.com/assets/UK-Faronics-FINAL-1.pdf

Räikkönen, I.A (2017), *Motivations behind employee information security behavior* (Master's dissertation, Technical University of Finland, Finland) Retrieved from https://pdfs.semanticscholar.org/3761/901d554605de8b122832e9de9a2f1d157731.pdf

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/

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

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).

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

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

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

Santillan, M. (2018) 75 Percent of Orgs Can't Effectively Detect and Respond to DataBreaches, 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/

SASRA (2018) The Sacco subsector 2018. Retrieved from: https://www.sasra.go.ke/index.php/regulation/theSaccosubsector#.XH4K74gzbIU

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

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

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

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/

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

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.

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/

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.

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

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

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/

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

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

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

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

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

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

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

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