European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) DOI: 10.7176/EJBM
Vol.11, No.27, 2019
www.iiste.org

Assessing the Current Status of Information Security Policies Among Saccos in Kenya

Jerotich Sirma[1*] Silvance O. Abeka[1] Benard Okelo[2]
1.School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, PO box 210-40601, Bondo,Kenya
2.School of Mathematics & Actuarial Sciences, Jaramogi Oginga Odinga University Science and Technology, PO box 210-40601, Bondo,Kenya

Abstract
In 2013, Communication Authority of Kenya (CAK) recorded cyber-attacks amounting to Sh5.4 million loses. In April 2016, Bandari Savings and Credit Cooperative Society lost Sh5 million through fraudulent ATM withdrawals (Nation Newspapers, April 8, 2016). These examples demonstrate weaknesses that may exist from security breaches and incidents caused by people, processes, and technology. Ministry of ICT and CAK are lacking specific Information Security Models tailored towards SACCOS in Kenya. The study therefore sought to assess the current status of information security policies among SACCOS in Kenya. The study adopted descriptive research design. The unit of observation was 135 SACCOS registered with SACCO Societies Regulatory Authority (SASRA) while the unit of analysis was 270 ICT personnel working in the 135 targeted SACCOS. The study targeted the SACCOS heads of IT department. The study used Nassiuma (2000) formula to get a sample of 85 respondents. Purposive sampling was further used in selecting study participants in every SACCOS who were considered to be knowledgeable of the variables under study. The study utilized questionnaire as the survey instrument to collect both quantitative and qualitative data. The study adopted descriptive statistics. Descriptive data was presented by use of frequency tables. The study established that in all the SACCOS studied, information security policy is used. However, there are still challenges on how information security breaches and incidents can be contained based on the results of the study and therefore calls for further research in academic research. The findings of the study indicate that SACCOS were able to validate that the enhanced information security model using an integrated approach worked as planned and reported to auditors, managers and executives that incident response programs are robust and reliable. If security controls didn't work as planned, they will need to fix them. The actions and resources needed should be included in in the report to executives in the SACCOS sector in Kenya
Keywords: SACCOS, Management controls, Information Security Policies, Risk assessment
DOI: 10.7176/EJBM/11-27-09
Publication date:September 30th 2019

1. Introduction

1.1 Background

SACCOS worldwide have been recognized as an important source of economic growth. Many people around the world are affiliated with co-operatives as reflected by International Cooperative Alliance (ICA Annual Report, 2016). Many countries that have achieved economic development have a dynamic and vibrant SACCOS' sector which contributes to the growth of those economies.

SACCOS also, provide savings and credit and investment opportunities to individuals, institutions and group members. SACCOS in Kenya have started to be more competitive in their field of financial institution since they contribute 30% of economic growth in the country (Gathurithu, 2011). As such, the SACCOS sector is still young in the adoption of information technology and thus is faced with myriad problems in addressing information security threats.

With the evolution of the Internet and networks in organization, there is an immediate need for current security measures and polices to reduce the threats and challenges emerging from new technologies namely software application and network devices (Alshboul, 2010). According to information security breaches survey (2015) conducted by Price Waterhouse Coopers (PWC) in collaboration with Info Security Europe (2013), indicate that the number of security breaches UK firms are encountering continue to increase. The rise in security breaches is mostly witnessed in small businesses which was only the case of large businesses.

Data security breaches in the U.S. is a growing concern for financial services companies due to the possible impact on customer service, lawsuits, loss of reputation, and regulatory penalties (Betz, 2016). The average cost of a breach the Association of Southeast Asian Nations (ASEAN) totaled $2.3 million. The Ponemon Institute (2017) also indicated that the cost associated with data breach varies by industry as well as geographical region. According to the study, some industries are more risky than others. In Australia for example, the financial sector suffered the largest cost of 380 Australian dollars, followed by services with 336 Australian dollars and technology with 274 Australian dollars. As a remedy to reducing the cost of data breach, companies globally

should establish incident response teams, use encryption techniques, appoint a chief information security officer to oversee the security program and participate in threat sharing and the most important feature is training employees.

Akuta, Ong'oa and Jones (2011) indicated that high levels of cybercrime are recorded in sub-Sahara Africa. The four countries include Nigeria, Cameroon, Ghana and South Africa. Kenya for example falls with the geography of sub-Sahara Africa where cyber threats are on the rise. According to Fihlani (2017) millions in South Africa were caught in the worst data breach where personal details of more than 30 million citizens was leaked on the internet hence placing them at a risk of identity theft. The information had 27GB file that contained names, full identity number, income, gender, employment history, contact numbers and even home addresses. According to CIO East Africa (2017), Cyber threats have since matured; syndicates have the potential to wreck devastating damages to institutions in terms of reputation, operations, finances and general data breaches.

According to Kenya Cyber Security Report (2016), lack of cyber security awareness among technology users puts Kenyan organizations in a critical challenge. Employees and customers have limited knowledge of the level of risk they are exposing themselves and their organizations. The approximate cost of cybercrime in Kenya has a high record of $175 million (Kenya Cyber Security Report, 2016). The motives for data breaches are increasingly financial. This obviously makes banks more of a target than ever.

According to Kenya Cyber Security Report (2016) more attacks targeting Kenyan banks ranging from insider threats to spear phishing and ransomware attacks were noted. Banks' vulnerability is realized through their web applications, Internet and Mobile banking platforms. While the attack vectors may differ, the execution of the attacks is often the same. It is important that local banks invest in mechanisms to Anticipate, Detect, Recover and Contain cybercrime (Kenya Cyber Security Report, 2016). SACCOS and microfinance institutions are also rapidly growing in Kenya. However, these organizations are focused on customer satisfaction and reducing costs that they tend to neglect investment in cybercrime prevention. This has made them a popular target for cybercriminals. Subsequently, serious threats of unauthorized users on the Internet, information security are facing huge challenges, and effective information security models for SACCOS are a major concern.

1.2 Statement of the Problem

Information security efforts will continue to be challenged by the rapid technological change and the increasing sophisticated nature of threats. While institutions are aware that the threat landscape is constantly evolving, they find it challenging to keep up with current developments amid competitive pressure to integrate new technologies into their financial institutions. In light of the challenges posed by new information security threats, SACCOS in Kenya are now responding to the fast changes in the financial environment and adopting new Information Technology (IT) approaches to the SACCOS' information security. In 2013, Communication Authority of Kenya (CAK) recorded cyber-attacks amounting to Sh5.4 million loses. Despite the high number, CAK indicated that a high number of cases are not reported, especially those involving banks. (Nation Newspapers, September 3, 2014). In 2015, the Directorate of Criminal Investigation's Banking Fraud Investigation Department (BFID) indicated fraud of Sh700 million by financial institutions in Kenya (Nation Newspapers, July 31, 2015). In April 2016, Bandari Savings and Credit Cooperative Society lost Sh5 million through fraudulent ATM withdrawals (Nation Newspapers, April 8, 2016). These examples demonstrate weaknesses that may exist from security breaches and incidents caused by people, processes, and technology. Ministry of ICT and CAK are lacking specific Information Security Models tailored towards SACCOS in Kenya. This study therefore proposed to develop an enhanced Information Security Model using an integrated approach to help SACCOS in Kenya to secure their environment.

1.3 Purpose of the Study

The aim of the study was to assess the current status of information security policies among SACCOS in Kenya.

1.4 Research Question

What is the current status of information security policies among SACCOS in Kenya?

2. Literature Review

2.1 Information Security Policies

Elements of information security include authenticity, accountability, non-repudiation and reliability. Subsequently, security policies provide guidance with regard to the physical and remote access to data of the SACCOS. Doherty and Fulford (2016) stated that information security policies should be in line with the SACCOS objectives. Verdon (2016) found out that countermeasures continue to surface due continued threats. After reviewing the potential threats to SACCOS network, the SACCOS Chief Security Officer (CSO) and/or Chief Information Officer (CIO) should develop, implement, and distribute a security policy or policies to all

employees. According to Whitman and Mattord (2013) and Greene (2016) an effective security policy must establish key goals for ensuring that authorized users can access the network and information resources. Additionally, the security policy must ensure employees know the penalties of inappropriate behavior when using SACCOS' information resources and/or assets. Within the policy, each SACCOS employee's information security responsibilities is to safeguard the integrity, confidentiality and availability of the SACCOS confidential data (Whitman & Mattord, 2013); Greene, 2016) that must be communicated. Metzler (2017) suggested using standards or security processes rather than just security policies to cater for the continued need to update the requirements as part of security policy maintenance. According to Metzler (2017), an organization stakeholders' involvement is critical in order to produce longevity and effective security policies.

For these security goals to be realized, SACCOS managing partners and IT personnel must be actively involved in developing these policies. If the security failure can be equated to a monetary figure, then the seriousness of developing an applicable security policy is more readily accepted by the managing partners (Greene, 2016; Whitman & Mattord, 2013). Security policies addresses the following topics: access control, acceptable use, business continuity and disaster recovery, change control management, confidentiality, data classification, data backup and recovery, disposal practices, e-mail practices, encryption, information protection, information systems security, Internet use, network security, privacy, physical security, remote access, system administration security, incident response, and termination (Greene, 2016; Metzler, 2017; Rotvold, 2014; Verdon, 2016). Metzler (2017) suggests developing a separate security policy for each topic in order to quickly update and approve procedures. Therefore, smaller separate documents rather than one large document would expedite revisions and approval of necessary revisions to the individual policy topics since they would be shorter and therefore easier to review.

With extensive explanation of rules on how the network can be accessed, with a concentration on maintaining confidentiality and identifying the ramifications of a security breach (Greene, 2016; Whitman & Mattord, 2013) is incorporated in the security policy of an organization. Distribution of the security policy to all SACCO's employees is very important. Security awareness is a topic all SACCOS' employees must understand so that their actions will not jeopardize confidential data in their possession (Alshboul, 2010). Therefore, SACCOS employees must be informed as to the applicable security policy pertinent to their job and understand why it is important to protect the information located on their computers from unauthorized access (Baker and Wallace, 2017; Chen, Shaw & Yang, 2016; Metzler, 2017).

Insider threats consisting of the disgruntled or curious employee must be addressed in the security policies to outline the ramifications of accessing data not relevant to the SACCOS employee's job description (Gupta & Sherman, 2012; Farn, Lin, & Lo, 2014); Lin, 2016). Insider threats are one of the most common causes of security breaches (Bowen, Hash and Wilson, 2016; Chen, Shaw and Yang, 2016; Ramim and Levy, 2016). Incident response procedures and the method for reporting information security incidents relative to insider breaches should be included in the SACCOS security policies (Chen et al., 2016). Attendance at security policy awareness training sessions on information security incident reporting should be required of all SACCOS' employees (Chen et al., 2016; Gupta & Sherman, 2012; Rotvold, 2014) on an annual basis. Rotvold (2014) suggests training attendance be a mandatory requirement incorporated into employee evaluations in order to assure enforcement of the security policy. Rotvold (2014) indicated that security policies compliance was first due to individual motivation, followed by responsibility in regards to information security and third is based on importance of information security. Thus, communication of the seriousness of information security responsibilities by SACCOS' management to SACCOS' employees is critical in building a culture wherein it is second nature for employees to apply security measures (Rotvold, 2014).

2.2 Status of Information Security Policies

According to Verizon Risk Team (2012) there is a possibility of SMEs being more often object to cyber-attacks because they are a part of supply chain or are business partners of big enterprises so perpetrators find easier to get to the big organizations through the small ones that are less well protected. This is why some large organizations approach SMEs and offer them help to deal with security in the cyber space (Arghandeh et al., 2016). However, as previously mentioned, despite of awareness for increasing trends of cyber-attacks on the global level, it is not easy to verify their number through the real statistics due to firms' reluctance to report them fearing to compromise themselves either in front of their clients or disbelieving these attacks are enough serious and dangerous.

2.3 Information Security

The information management system and e-business technology systems and the networks, used for generating, storing and retrieving information and the human beings are important business assets of every organization. The security, integration and availability of information are essential for any banking organization to maintain its competitive edge, cash flow, profitability, legal compliance and commercial image. The application of

Information Technology has brought about significant changes in the way the banking and the financial organizations process and store data. The telecommunication networks have played a catalytic role in the expansion and integration of the Information Systems, within and among the organizations, facilitating data accessibility to different users. This has made it imperative for each organization to put in place adequate security controls to ensure data accessibility to all the authorized users, data inaccessibility to all the unauthorized users, maintenance of data integrity and implementation of all security threats to guarantee information and information systems security across the organization. This makes it necessary for each organization to define, document, communicate, implement and audit Information Systems Security (Information Technology, 2015).

Securing data is a key function of IT and business strategies. Information security is the practice of protecting technology systems and data from vulnerabilities, threats, and attacks. The vulnerabilities, threats, and attacks can be an intentional or unintentional exploitation of systems to compromise the availability, integrity, and confidentiality of information. Information security vulnerabilities and threats are present in technology innovations; therefore, an analysis of organizational risk should include information security parameters (Ioannidis, Pym, & Williams, 2012).

Susanto, Almunawar, and Tuan (2011) noted that information security assessments are essential in every business environment. Security professionals need to develop frameworks to guide the practical and theoretical security practices within the organization (Susanto et al., 2011). The frameworks above may assist business leaders in understanding best practice security models. The dependence on technology innovations by businesses, governments, and individuals is on the rise (Susanto et al., 2012). Innovations such as the Internet have made business transactions such as banking, job searching, and shopping convenient for many individuals (Lawrence, 2011). Companies are using IT solutions to improve and streamline business processes (Susanto et al., 2012), and technology has become an enabler of organizational agility (Whitman & Mattord, 2014).

The principal objective of information security is to maintain the availability, integrity, and confidentiality of information (McIlwraith, 2016). As information security continues to be a problem for organizations, offsetting data security against accessibility has proven to be a prevalent problem. Businesses operate in a technology driven era where information saved on computers and network devices are vulnerable to security attacks. Data security breaches are a result of inefficient management of the availability, integrity, and confidentiality of information. The effective management of information security can alleviate security vulnerabilities for both external and internal entities (Liao and Chueh, 2012). Maintaining the integrity and confidentiality of information, and ensuring data availability to users is a challenge for many organizations.

Harris and Patten, (2014) states that security can be defined as the state of being free from danger and not exposed to damage from accidents or attack, or it can be defined as the process for achieving that desirable state. The objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed. Business is becoming increasingly dependent on technology and the internet to the point where some businesses would come to a screeching halt if they did not have it. This is particularly true in larger companies, where the ability to communicate and access information is the lifeblood of the business. The internet provides an effective, immediate and powerful method for organizations to communicate on all sorts of issues. This exposes all these organization to the security risks that go with connection to the internet.

According to (Thompson and Kaarst-Brown, 2015; Wu and Rocheleau, 2011; Yukl, 2016) cyber security incidents and breaches, most institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years. The attempted methods ran the gamut, with most institutions reporting incidents involving malicious software (malware) (22%), phishing (21%), pharming (7%), and botnets or zombies (7%). The larger the institution, the more likely it appeared to experience malware and phishing attempts. About 13 percent of small institutions reported being attempted targets of malware, as compared to 21 percent of medium institutions and 35 percent of large institutions (Loeber, 2014). Similarly, about 16 percent of small institutions reported attempted phishing, as compared to 22 percent of medium institutions and 33 percent of large institutions.

2.4 Information Security Risk Assessment

An information security assessment is important in protecting the confidentiality and sensitivity of data (Humphreys, 2007; Salmela, 2008) that resides on a SACCOS' network and portable media devices (Heikkila, 2007). A security assessment based on a combination of a risk assessment that identifies the potential threats pertaining to assets of a SACCOS, along with vulnerability scans of applications, ports, and operating systems, including mission critical databases, assist in the mitigation and remediation of potential threats (Moga, Nor & Mitrica, 2012). Based on the identification of the mission critical assets that need the utmost protection and the level of risk accepted by SACCOS management, the scope of the vulnerability assessment is defined (Humphreys, 2007; Salmela, 2008).

The risk assessment should include the review and analysis of compliance with information security

policies and procedures by SACCOS' employees. Participants in the risk assessment process can include those users that remotely access SACCOS content and information. The various assets of a SACCOS must be evaluated to determine what the critical assets are and whether or not they are adequately protected (Humphreys, 2007). NIST outlines the various levels of management controls, operational controls, and technical controls that an organization should strive for with its security plan (Bowen et al., 2006). It is important to begin with the mission critical components and develop policies to mitigate any gaps between security risks and corrective actions (Humphreys, 2007).

Threat identification includes reviewing the physical or hardware and software components that support access to the SAACOS' computer systems and network and any vulnerable applications which may perpetuate a security breach incident. Each threat is ranked by the probability of occurrence and whether or not a SACCOS is willing to accept the risk, avoid the risk by prohibiting a certain action from being taken, or transfer the risk to an insurance carrier or other third party (Humphreys, 2007; ISO/IEC 27001 Joint Technical Committee, 2013). Threat probability levels assist with the control analysis, likelihood of occurrences, and impact analysis determination that must be made for each asset (Bowen et al, 2006; Humphreys, 2007).

Based on the risks that are identified, the SACCOS should consider implementing controls to mitigate the threats and vulnerabilities. Care must be exercised when performing vulnerability scans of SACCOS networks. The potential for exposing a firm's assets during the vulnerability assessment should be determined and guarded against unintended intrusions (Bowen et al., 2006). Management controls, operational controls, and technical controls, safeguard tangible and intangible assets. A SACCOS' reputation and client perceptions are intangible assets (Desouza, 2008). Tangible assets include SACCOS' hardware, software, electronic documents, paper documents, and employees (Humphreys, 2007).

2.5 Research Gap

Various studies have been conducted on the status of information security policies for example a study by McConnell and Hamilton (2002), Whitman and Mattord (2013), Greene (2006), have shown that information insecurity has affected the way financial institutions conduct their daily operations online. The study by Heiser (2004) shows a growing trend and sophistication of cyber-attacks, a record of 46 percent of respondents identified information security as the top concern, according to The Depository Trust and Clearing Corporation's (DTCC). The information security ranking is nearly doubled compared to DTCC's Systemic Risk Barometer Study in March 2014 where 24 percent of respondents cited cyber security as the number one threat.

The studies by Thompson and Kaarst-Brown (2005); Wu and Rocheleau (2001); and Yukl, (2006) show that there are increased information security breaches and incidents. Most institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years. The attempted methods ran the gamut, with most institutions reporting incidents involving malicious software (malware) (22%), phishing (21%), pharming (7%), and botnets or zombies (7%). Siponen and Oinas-Kukkonen (2007) study show that research has historically concentrated on the technological perspective; and additional research is needed with regard to practical observations of security management. In a study of companies in Norway, Hagen, Albrechten, and Hovden (2008) determined security measures are interdependent. Hagen et al. (2008) also studied the implementation, effectiveness of security measures, which resulted in an inverse relationship, and the inverse relationship was interpreted as a metaphorical staircase of four steps: security policy; procedures and control; tools and methods; and awareness creation.

Doherty and Fulford (2005), Wiant (2005), and Heikkila (2009) studies explored the relationship between security policies and data security breaches, and the findings of all three investigations demonstrated that there was no statistically significant relationship between having a security policy and realizing a reduction in data security breaches. These studies indicate that an organization can have a security policy in place, which do not prevent or reduce incidents and security breaches.

However, other studies have developed general frameworks and models on information security that are best utilized by large organizations and large financial institutions but SACCOS in Kenya who are new to IT still lack an effective information security model that addresses its information security threats. This study therefore developed and tested an enhanced Information security model using an integrated approach by adapting in part Doherty and Fulford conceptual framework and John Boyd OODA Loop model that aid SACCOS in Kenya to address its information security breaches and incidents.

2.6 Conceptual Framework

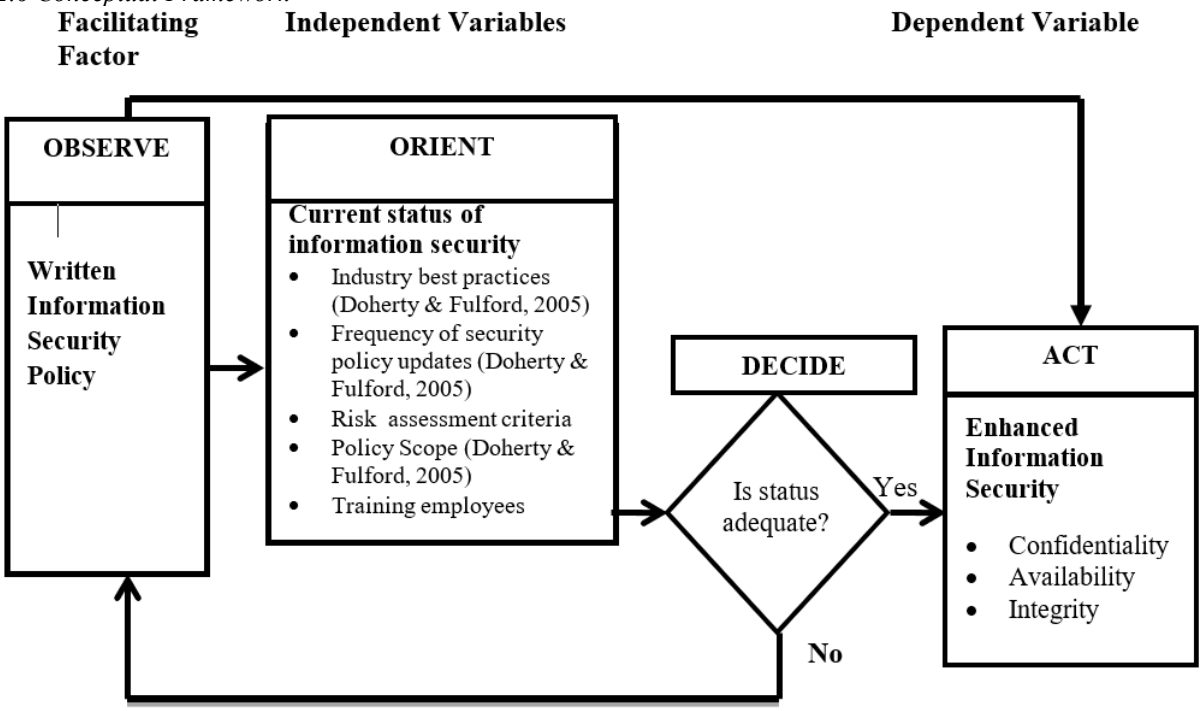

Figure 1: Conceptual Framework
Source: Adopted in part by Doherty and Fulford (2005) and John Boyd OODA Model

3. Research Methodology

3.1 Research Design

The study adopted descriptive research design. The descriptive studies sought to obtain information that describes existing phenomenon by asking individuals about their perceptions, attitudes and values.

3.2 Study Population

The unit of observation was 135 SACCOS registered with SACCO Societies Regulatory Authority (SASRA) while the unit of analysis was 270 ICT personnel working in the 135 targeted SACCOS. The study targeted the SACCOS heads of IT department.

3.3 Sample and Sampling Techniques

The sample size of 85 SACCOS was obtained by using coefficient of variation. Nassiuma (2000) contends that in most surveys, a coefficient of variation in the range of 21%≤C≤30% and a standard error in the range of 2%≤e≤5% is acceptable. The study therefore used coefficient variation of 30% and a standard error of 2%. Nassiuma (2000) formula is as follows:

$n= Nc^2/ (c^2 + (N-1) e^2)$

Where: n = sample size

N= accessible population

c= Coefficient of Variance

e= standard error

$n=135x0.3^2/0.3^2 + (135-1) 0.02^2 = 84.61$

Simple random sampling was used to select 85 SACCOS that are registered with SASRA. Purposive sampling was further used in selecting study participants in every SACCOS who were considered to be knowledgeable of the variables under study.

3.4 Instruments of Data Collection

The study utilized questionnaire as the survey instrument to collect both quantitative and qualitative data and to document responses from 85 IT personnel who were purposively selected from 85 SACCOS in Kenya who are registered with SASRA. The pilot study sample was drawn from Egerton University SACCO Society Ltd, Skyline SACCO Ltd, Boresha SACCO Society Ltd, Cosmopolitan SACCO Society Ltd and Wareng Teachers SACCO Society Ltd. Convenience sampling was used to identify the SACCOS under the pilot study. A pilot test was carried out to test the validity of the survey instrument, where content validity was employed, which

measured the degree to which the test items represent the domain or universe of the trait being measured. Items were randomly chosen from the content that was accurately represented by the information in all areas. The study obtained a group of items which was representative of the content of the trait or property to be measured. The pilot study also tested the clarity of instructions; relevance, terminology used, comprehensibility, and time it took to administer one survey questionnaire. Criterion validity was done to determine the ability of the questions to make accurate prediction.

3.5 Data Analysis and Presentation

Data collected from the research was coded and analyzed using descriptive statistics which were derived from statistical package for social sciences (SPSS). Qualitative and quantitative methods of data collection were used. Quantitative data collected during the research explained the phenomenon being analyzed and it was presented using descriptive statistics which included percentages, mean, standard deviation, frequency distribution tables, graphs and pie charts.

4. Findings

4.1 Response Rate

A total of 85 questionnaires were distributed to IT employees from 85 SACCOS that are registered with SASRA in Kenya. Out of the 85 questionnaires issued to respondents, only 72 were successfully completed and returned for analysis hence giving the study 84.7% response rate. Nine questionnaires were incomplete and were omitted from the analysis and four SACCOS from the sample size refused to participate in the study.

4.2 Demographic Information

Table 1. Age of the participants

Age	Frequency	Percent
20-30	32	44.4%
31-40	34	47.2%
41-50	6	8.3%
Total	72	100.0%

Table 1 displays the age of the respondents. 44.4 % of the respondents aged beween 20-30, 47.2% are aged between 31-40 years, 8.3% of the participants aged between 41-50 years. The study reveals that majority of the participants are below 40 years which provides the institution with a younger and innovative minds to provide strategies for security measures in information security.

4.2.1 Education level of the Respondents

Table 2. Education level of the Respondents

Level of Education	Frequency	Percent
Diploma	15	20.8
Bachelor degree	47	65.3
Masters	9	12.5
Prefer not to answer	1	1.4
Total	72	100.0

Table 2 shows the level of education of the respondents. The majorities, 65.3% of the respondents have Bachelor degrees, 20.8% are Diploma holders, and 12.5% are Master's degree holders while 1.4% preferred not to answer. The study reveals that 65% of the participants have a Bachelor degree which provides the institution with learned personnel who can apply the knowledge gained in academia regarding strategies for security measures in information systems.

Table 3. The number of years worked in the Institution

Number of years worked	Frequency	Percent
Less than 1 year	6	8.3%
Between 1 and 2 years	7	9.7%
Between 2 and 3 years	21	29.2%
Between 3 and 4 years	9	12.5%
Above 4 years	29	40.3%
Total	72	100%

Table 3 shows the number of years the respondents have worked. 8.3% of the respondents have worked for less than 1 year, 9.7% have worked between 1 and 2 years, 29.2 % have worked for 2 to 3 years, 12.5% have worked for 3 to 4 years while 40.3% have worked for 4 years and above. The study reveals that the institution has high-qualified personnel to provide professional guidance to the implementation of the various security strategies in the institution. The study findings concurs with the findings by (Johnson & Warkentin, 2008) who

stated that professional guidance is required by the institutions in order to develop measures that can be used to enhance security within the organization information systems.

4.3 Descriptive Findings and Discussions

4.3.1 Information Security Technologies used by SACCOS

Table 4: Information Security Technologies used by SACCOS

Security Technology	Percentage
Access control	97%
Endpoint control	88%
Network control	98%
Host control	96%

Under current status of information security among SACCOS, respondents were asked to indicate information security technologies used by SACCOS that decreased security breaches and incidents. Table 4.8 presents the responses and percentages for the security technologies used by SACCOS. Over 90 percent of the SACCOS use access control, network control and host control. For several decades, network security was the main layer of defense for computer systems against malicious software and hackers (McIlwraith, 2006). According to McIlwraith, (2006), network security alone has proven to be an inadequate line of defense against security threats and vulnerabilities. 88 percent of the SACCOS utilized endpoint control.

The security technologies utilized by SACCOS according to the study findings reduced computer viruses, hacking incidents and unauthorized access to use data (see table 4.8), thereby decreasing security incidents and breaches. IT security provides protection of informational assets for companies. Examples of IT security are access controls, endpoint controls, network controls, and host controls. Organizations can achieve information security by implementing an applicable set of controls. These controls are selected through the chosen risk management process and managed using an Information Security Management Standard (ISMS), including processes, procedures, organizational structures, software and hardware to protect the identified information asset.

4.3.2 Current status of information security among SACCOS

Table 6: Current status of information security among SACCOS

Factors	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The security policy of our organization reflects the business objectives	0%	0%	2.8%	58.3%	38.9%
	0	0	2	42	28
The approach to implementing security is consistent with the SACCOS culture	1.4%	5.6%	16.7%	48.6%	27.8%
	0	4	12	35	20
There is a visible commitment from the management towards information security	1.4%	0%	4.2%	47.2%	47.2%
	1	0	3	34	34
There is a good understanding of security risks and requirements among SACCOS employees	0%	0%	1.4%	29.2%	69.4%
	0	0	1	21	50
There is adequate distribution of guidance on IT security policy to all SACCOS employees.	0%	0%	4.2%	43.1%	52.8%
	0	0	3	31	38
SACCOS provide appropriate training and education to all employees	5.6%	0%	18.1%	48.6%	27.8%
	4	0	13	35	20
The organization have put in place a comprehensive measurement system for evaluating performance in security management	1.4%	1.4%	19.4%	44.4%	33.3%
	1	1	14	32	24
There is a visible commitment from management towards information security	1.4%	4.2%	19.4%	43.1%	31.9%
	1	3	14	31	23

Table 6 presents the responses and percentages for the importance of best practices success factor on IT security implementation in SACCOS. In ensuring security policy reflects business objectives, 58.3% of the respondents found it very important to the operations of their SACCOS. 48.6% of the respondents deemed very important for their SACCOS to implement security that is consistent with their culture. An organization that aims to cultivate an acceptable level of an information security culture would require a single, all-encompassing (considering all the relevant focus areas from the current research approaches) approach that can be used in organizations from any environment or of any size. The findings agreed with Betz, (2017) who found out the identification of the information assets of the company are a critical success factor for the efficient and effective implementation of information security in companies.

The respondents also reported that 47.2% found it very important and extremely important to have commitment from management regarding adoption of industry best practices. This agree with Mishra (2015)

who found out that business managers need to evaluate the positive and negative effects of technology on an organization as a measure of normal business activities**,** 69.4% of the respondents indicated the extreme importance of a good understanding of security requirements by SACCOS employees. Effective marketing of security to all SACCOS' employees or other members of the SACCOS had the highest score of 48.6% in terms of importance. 44.4% of the respondents reported that it was very important to distribute guidelines on IT security policy to all SACCOS' employees or other members of SACCOS. Over half of the respondents (56.9%) found extremely important to provide appropriate training and education to all SACCOS' employees and other members. Comprehensive measurement system for evaluating performance in security management had 50% of the respondents reporting the factor as very important. 43.1% of the respondents deemed very important in provision of feedback system for and education to all employees or other members of SACCOS. Financial institution such as SACCOS need a systematic information security approach that is used for the arrangement or structuring of information security components to implement information security in an effective manner to mitigate risks in an organization. An information security component is considered as a part of an information security approach that contributes to the implementation and maintenance of information security.

5. Conclusion

The study established that in all the SACCOS studied, information security policy is used. The respondents did not oppose to the use of information security policy when they perform SACCOS daily tasks. This is a clear indication that information security policy will continue to guide SACCOS in running information technology operations within the sector. However, there are still challenges on how information security breaches and incidents can be contained based on the results of the study and therefore calls for further research in academic research. Furthermore, although information security policies are practiced within the SACCOS sector, there are still rampant security breaches and incidents recorded. Updating security policies within a shorter period, using adequate security measures and complying with industry best practices can aid SACCOS in reducing security breaches and incidents.

6. Recommendations

The findings of the study indicate that SACCOS security policies need to be reinforced as planned and reported to auditors, managers and executives that incident response programs are robust and reliable. If security controls didn't work as planned, they will need to fix them. The actions and resources needed should be included in in the report to executives in the SACCOS sector in Kenya

References

Akuta, E., Ong'oa, I. & Jones, C. (2011). Combating Cyber Crime in Sub-Sahara Africa; A on Law, Policy and Practice,' *Journal of Peace, Gender and Development* 1(4),129-137.

Alshboul, A. (2010). Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks. *Communications of the IBIMA,* 2010:1-9.

Arghandeh, H., Carmo, D., Sergio, T., Carvalho, G., & Murta, O. (2016) '' Runtime Monitoring and Auditing of Self-Adaptive Systems'', 11th *IEEE International Conference on Global Software Engineering* (ICGSE), Brazil

Baker, W., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1), 36-44.

Bowen, P., Hash, J. & Wilson, M. (2006). *Information security handbook*: A guide for managers. NIST special publication 800-100. Retrieved from http://csrc.nist.gov/ publications/nistpubs /800-100/SP800-100-Mar07-2007.pdf

Chen, H., Chen, H., Shaw, C., & Yang, L., (2015). How can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions. ACM Trans. Internet Technol., 3(1):28–48, February 2003. 3, 4.

Desouza, K. (2008). The neglected dimension in strategic sourcing: security. *Strategic Outsourcing: an International Journal*, 1(3), 288-292.

Doherty, M., & Fulford, H.(2015) Self-adaptive software: Landscape and research challenges," ACM TAAS, vol. 4.

Farn, J., Lin, K., & Lo, C-C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interface*, 30(1), 1-7.

Gathurithu, A. (2011). An investigation into the factors affecting marketing of Sacco products in Thika, Kenya. *A research project submitted at Makerere University, Uganda*.

Greenleaf, G. (2012). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report, Issue 115. Queen Mary School of Law Legal Study Research Paper No. 98/2012.*

Gupta, T., & Sherman, G. (2012). Determinants of Data Breaches: A Categorization-Based Empirical

Investigation, *Journal of Applied Security Research*, 7(3), 375-395.
Hagen, J. M., Albrechten, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
Harris, F., & Patten, Y. (2014) Non-functional Properties in Software Product Lines: *A Taxonomy for Classification''*, In Proceedings of "SEKE'12", 663-667
Heikkila, F. (2009). An analysis of the impact of information security policies on computer security breach incidents in law firms (Doctoral dissertation). Available from Pro Quest Dissertations and Theses database. (UMI No. 3380050)
Humphreys, E. (2007). *Implementing the ISO/IEC 27001: Information Security Management System* Standard, Boston, M.A: Artech House
ICA Annual Report (2016). The 2016 International Summit of Co-operatives. Retrieved from https://www.ica.coop/sites/default/files/publication-files/enannual-report2016final-681195095.pdf
Information security breaches survey (2015). Retrieved from Information superhighway. Information Management & Computer Security, 5(1), 20-22.
Kenya Cyber Security Report (2016). Achieving Cyber Security Resilience: Enhancing visibity and increasing awareness. Retrieved from http://www.serianu.com/ downloads/Kenya Cyber Security Report2016.pdf
Lawrence, V. (2011). "Comparison of Adaptive Information Security Approaches'', ISRN Artificial Intelligence, Article ID 482949, (3) 18
Loeber, A. (2004). Practical wisdom in the risk society. *Methods and practice of interpretive Analysis on questions of sustainable development. PhD diss., University of Amsterdam*.
McConnell, W., & Hamilton, F., (2002). Managing Information Risks and Protecting Information Assets in a Web 2.0 era. In: 23rd Bled e-Conference Trust, Implications for the Individual, Enterprises and Society. Bled, Slovenia 20-23 June 2010
McIlwraith, A. (2006). Information security and employee behavior. *How to reduce risk through employee education, training and awareness*
Metzler, M. (2007). Promoting security policy longevity. *Computer Security Journal. XXIII*, 2(3), 82-94.
Moga, M., Nor, K., & Mitrica, E. (2012). E-banking Adoption in Romanian Companies: Determining Factors and Model, IBIMA Publishing. Retrieved from http://www.Ibimapublishing.com/journals/CIBIMA/2012/385699/385699.pdf
Nassiuma D. (2000). Survey Sampling: Theory and Methods. University of Nairobi Press, Nairobi.
Ramim, M. & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.
Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology*, 23(3), 185-202.
Siponen, T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database,* 38(1), 60-80
Thompson, C., & Kaarst-Brown, K. (2005) Computer Security training and education: A needs analysis. Oakland, CA, USA, pp. 26-7.
Verdon, D. (2006). Security Policies and the software developer. *IEEE Security & Privacy*, 4(4), 42-49.
Whitman, M. & Mattord, H. (2013). Management of Information Security **(**4th edition) Boston, MA: Cengage Learning
Wiant, R. (2005). A lesson in risk management. Insurance Networking News, 16(5), 24-26
Wu, Y. & Rocheleau, E., (2001). Information security policy – what do international information security standards say? Computers & Security, 21(5), 402-409.
Yukl, J., (2006). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246-260.