International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

To Investigate the Strength of Existing Information Security Policies among SACCOS in Kenya

Jerotich Sirma[1], Silvance O. Abeka[2], Benard Okelo[3]

[1, 2]School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, P.O. Box 210-40601, Bondo, Kenya

[3]School of Mathematics & Actuarial Sciences, Jaramogi Oginga Odinga University Science and Technology P.O. Box 210-40601, Bondo, Kenya

Abstract: ***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 sought to assess the strength of existing information security policies among SACCOS in Kenya. The study adopted descriptive studies. 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 size 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 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.The study adopted descriptive statistics. Descriptive data was presented by use of frequency tables. The study concluded that breaches among SACCOS for the last two years as a result of hacking incident, natural disaster, and damage by disgruntled employee have been somewhat insignificant. The study further concluded that security incidents and breaches are under reported. From the conclusion the study concluded that SACCOS need to reinforce training of its employees and strengthen their policies to achieve enhance information security. To ensure the security of information systems and data, financial institutions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure.***

Keywords: SACCOS, Management controls, Security policies, Security risk assessment

1. Introduction

1.1 Background

SACCOS also, provide savings and credit and investment opportunities to individuals, institutions and group members. 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 economicdevelopment have a dynamic and vibrant SACCOS' sector which contributes to the growth of those economies.

Global trends in cybercrimes demonstrate that the financial sector is the sector most targeted by cyber criminals. Their activities include phishing, identity theft and the creation of fake banking applications. The United Nations Office of Drugs and Crime (UNODC) estimate that identity theft is the most profitable form of cybercrime, generating perhaps US$1 billion per year in revenue on a global basis. 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.

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. Earlier on, cyber security threats were limited to phishing, user access, and some aspects of data manipulation. The threats are now a great disaster to many organizations. Hackers are also having a desire to attack small businesses (SMEs) because of their unpreparedness.

Since SMEs are small in size based on their businesses, they tend to falsely believe that they are encapsulated from attacks due to their small nature. With their innovative nature and growing customer acquisition makes them attractive prey to hackers. Unknowingly, some of them may actually offer that gateway to attack multinationals as they are often subcontracted to offer services to the big Corporations. Subsequently, no one is immune to cyber-attacks. They include breach of privacy and security of personally identifiable information, stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on computers, posting confidential business information on the Internet, with the potential for disrupting a country's critical national

infrastructure (CIO East Africa, 2017). According to Kenya Cyber Security Report (2016) more attacks targeting Kenyan banks ranging from insider threats to spear phishing and ransom ware 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 an effective information security model for SACCOS is 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 sought to determine the strength of existing information security policies among SACCOS in Kenya.

1.3 Purpose of the Study

The aim of the study was to determine the strength of existing information security policies among SACCOS in Kenya.

1.4 Research Question

What is the strength of existing information security policies among SACCOS in Kenya?

2. Literature Review

2.1 Systems Theory

The study was anchored on systemstheory. The theory was developed by vonBertalanffy in the 1940s, systems theory relates to the concept of an organism as an open system with various components working together to complete a task (von Bertalanffy, 1968). A system has inputs and outputs working together to achieve the objectives of the system (von Bertalanffy, 1968). Furthermore, von Bertalanffy (1968) indicated that a system is a mechanistically oriented object evaluated solely in terms of mathematics, feedback, and technology. Von Bertalanffy utilized systems theory to demonstrate that living systems are open hierarchical systems aimed at achieving a state of equilibrium.

Hammond (2010) further elaborated on von Bertalanffy's systems theory as the foundation of the open-systems concept stating that all components of an organizationmust function properly to accomplish business objectives. As business leaders continue to take advantage of technology, they need to ensure organizational components are working together (Hammond, 2010). Further, Mangal (2013) utilized systems theory to predict whether new website features improved user efficiency or improved system functionality. Mangal stated that websites with dysfunctional components were less efficient and affected a user experience, and a cohesive integration of system components provides for an enjoyable experience. In relation to systems theory, the integration and collaboration of all information security elements within an organization is essential to minimize security threats effectively.

2.2 Strength of existing information security policies

Rastogi and Von Solms (2016) define that "information security governance consists of the frameworks for decision-making and performance measurement that Board of Directors and Executive Management implement to fulfill their responsibilities of providing oversight, as part of their overall responsibilities for protecting stakeholder value". This definition of information security governance term will be used as reference in this paper because more comprehensive and suitable for this research work. The main purpose of information security governance implementation is to protect the most valuable asset of an organization.

The identification of the information assets of the company is a critical success factor for the efficient and effective implementation of information security in companies. Betz, (2017) categorize the information assets to be protected in the banking industry into four items which are: a) Insider information: Information which gives its possessors an unlawful market advantage and is suitable for the carrying out of insider operations (for example: board of directors' meeting minutes, capital market information, and internal company financial data); b) Client information: information which makes the inference of the identity of the client possible (for example: name, address, date of birth) including the designation of his bank contact information (account number, deposit number); c) Numbered account

client information: Client information of an economic beneficiary or assignee of numbered or imaginary accounts.

Security governance is a challenge for business leaders, as ISG involves adequate risk management, reporting, and accountability. ISG is an essential component of IT governance and as a result information security has become an integral part of organizational management (Yaokumah, 2014).The establishment of ISG programs begins with risk identification and assessment, also to business and technology risk management (Yaokumah,2014). Understanding security risks may ensure an ISG team can properly implement ISG initiatives.Effective ISG teams provide firms with the ability to manage information securityat the executive level and bring security to the attention of the board of directors andCEO's (Whitman &Mattord, 2013). Further, Whitman and Mattord (2013) noted that ISG teams assist information security leaders with planning processes to ensure inclusionof desired goals and objectives for organizational security policies. Nevertheless, tomaintain an ISG program, security experts, and managers need to be able to quantify theROI of the program to the organization (Whitman & Mattord, 2013).

According to Yaokumah, (2014) advances in targeted security threats have been increasing over the last decade. The increased number of mobile and portal devices means businesses must develop ISG programs that can adapt to evolving threats. Nicollet indicated that in 2015, approximately 80% of all security compromises would exploit well-known security flaws and vulnerabilities detectable by a security monitoring system. Furthermore, Nicollet advocated the need for security experts to work hand-in-hand with technology innovators and professionals to assess security vulnerabilities. This collaboration ensures security programs are up-to-date with information on known and unknown threats.As technology leaders work on developing ISG programs, incorporation of best practices and integration with business goals are essential. According to Mishra (2015), security governance defines the direction of information security policies and practices with an organization. Business managers need to evaluate the positive and negative effects of technology on an organization as a measure of normal business activities (Mishra, 2015). The Internet, for example, has facilitated the development of vast communication networks linking businesses and individuals, as well as introducing new security threats. As a result, governments have ratified information security laws and regulations to increase accountability and protect consumers and proprietary data (Chen et al., 2015). The number of security breaches in the United States hasincreased each year, despite additional efforts to safeguard consumer data fromcompromise. The U.S. government and others entities around the world are focusing onprotecting computer networks and data through laws, regulations, and industry technology initiatives.

The integration of technology in a global economy has proven to be beneficialand sometimes disastrousfor businesses. In a global environment, decisions, policies, and regulations by governments such as the United States and the European Union affect the global market. The standards, rules, and regulations set by developednations have become the framework for underdeveloped nations. Compliance withgovernment regulations by businesses is an essential element of theSecurity implementation process (Moshirian, 2011).

Maintaining compliance with industry and government security regulations suchas the NIST Special Publication 800-144 is a challenge for most companies (Chen et al., 2015). U.S. corporations have invested in internal and external security controls, andaudit processes to ensure compliance with government and industry regulations.

However,Wallace et al. (2011) noted that effective security management strategies could assistbusinesses with uninterrupted SOX compliance.For decades, the United Kingdom, like other developed nations, has enactedregulations aimed at dealing with the growing issues of data loss and privacy. In 2010, the U.K. House of Commons passed the Digital EconomyAct (DEA) with the goal to protect individual privacy, copyright infringement, and dataloss (Mansell and Steinmueller, 2013). Laws andregulations such as DEA provide business and individual's protection.Many states in the United States have passed data security breach and notificationlaws. The State of California led the legal battle with one of the toughest notification laws(Betz, 2017).

In 2002, the California state legislature passedthe California Security Breach Information Act (SB-1386), which required businessesstoring personal information to notify individuals in the event of an information securitycompromise (Legislative Counsel of California, 2002). The California Security BreachInformation Act stated that information such as first and last names, social securitynumbers, driver's license numbers, bank account numbers, and credit/debit card numbersare personal and confidential information.
According to Burdon, (2011) California's legislative bodyconsidered SB.1386 as a possible remedy for identity theft. The bill empoweredconsumers seeking damages from businesses in the event of a breach of consumers'personal information, as well as an early notification process to allow consumers tocancel accounts, and notify the credit bureau to prevent potential fraud. The notificationlaw in California required businesses to implement notification triggers, notificationmechanisms, and strategies to enforce, respond, and mitigate security threats. The globalization of industries has introduced new businesses opportunities and challenges. Transporting, sharing, storing, and transmitting sensitive information, such as banking data, between countries has introduced new concerns for multinational corporations (Burdon, 2011).

Risk management is a business strategy aimed at developing business environments for a limited probability of events that may cause damage to an organization's assets. According to Chitakornkijsil (2010), riskmanagement is the process through which an organization identifies business risks and losses to developing a strategy to discover, minimize, and respond to future risks. However, the risk is uncertain, and there are different methods for defining and identifying potential business losses. Identifying situations, where the loss is probable, is the objective of risk management. Chitakornkijsil also noted that risk

management is complex and adds value to an organization and may promote competitive advantage.

According to Patil et al. (2012), business managers and technology leaders need to understand business risk and information asset vulnerabilities.Business leaders take risks with the introduction of new products, expansion ofnew markets, reorganization of executive management, and the acquisition of other firmsto increase shareholder wealth. However,organizational mismanagement, such as the collapses of Lehman Brothers Holdings andWorldCom, indicated the need for effective risk management within corporategovernance. Patil et al. (2012) noted thatcorporate boards and executives are concerned about and proactive towardsorganizational exposure to risks. High level of organizational risk means governance andstrategies need to be flexible, iterative, and inclusionary as well as focus on risk mitigation, avoidance, and acceptance (Patil et al., 2012).

The efforts by organizations to mitigate informationsecurity threats through a risk management approach consider the strategic valueof information assets. An effective management security plan requires both business andtechnology leaders to accept the possibility of the unknown. In addition, security expertsneed to have effective risk management skills to ensure proper identification of businessrisk posed by technological innovations (Amancei, 2011).Organizationsface many types of security threats and vulnerabilities. Informationsecurity risk management has become an integral part of firms' business strategies. Bojanc and Jerman-Blazic (2013) stated thatorganizational security risks include the inadvertent disclosure of sensitive andproprietary business information by employees. Moreover, managing the risks associatedwith inadvertent disclosure of sensitive information is a concern for organizations,especially with the prevalence of social media (Borison& Hamm 2010).

2.3 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).

2.4 Research Gap

The studies 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.

2.4 Conceptual Framework

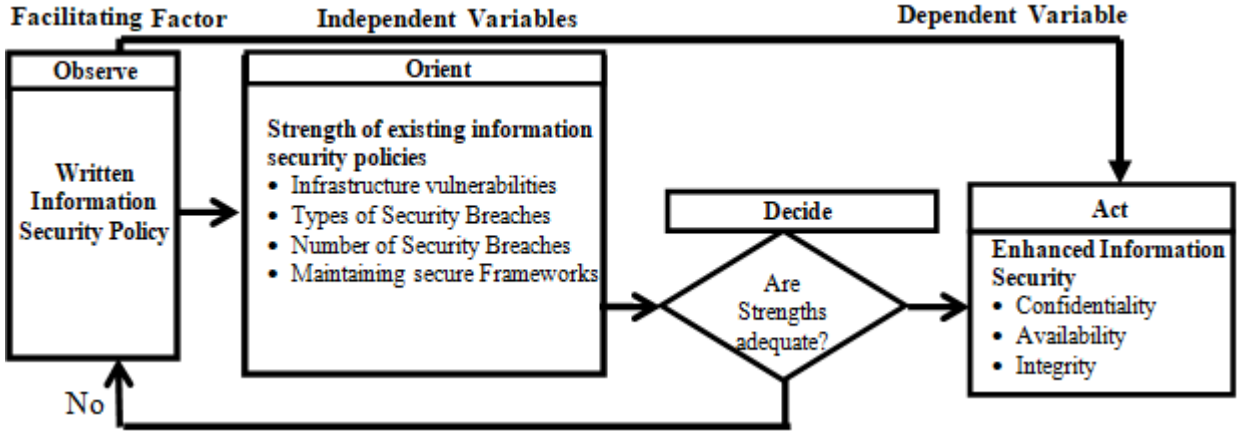

Figure 1*:* Conceptual Framework
Source: Adopted in part by Doherty and Fulford (2005) and John Boyd OODA Model

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 wererandomly 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

4.2.1 Education level of the Respondents

Table 1: 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 1 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.

4.2.2 The number of years worked in the Institution

Table 2: 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 2 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 Security Threats Occurrences in the Last two Years

Table 3: Security Threats Occurrences in the Last two Years

Type of Breach	0	1-5	6-10	11-14	>14	Mean	Std
Computer viruses	55.6%	20.8%	18.1%	5.6%	0%		
Frequency	40	15	13	4	0	2.19	0.929
Hacking incident (external)	91.7%	8.3%	0%	0%	0%		
Frequency	66	6	0	0	0	1.08	0.278
Unauthorized access to use of data (internal)	68.1%	29.2%	2.8%	0%	0%	1.35	0.535
Frequency	49	21	2	0	0		
Theft of hardware software	77.8%	20.8%	1.4%	0%	0%		
Frequency	56	15	1	0	0	1.24	0.459
Computer-based fraud	61.1%	36.1%	2.8%	0%	0%		
Frequency	44	26	2	0	0	1.42	0.550
Human error	36.1%	36.1%	20.8%	1.4%	5.6%		
Frequency	26	26	15	1	4	2.04	1.067
Natural disaster	68.1%	29.2%	2.8%	0%	0%		
Frequency	62	9	1	0	0	1.15	0.399
Damage by disgruntled employee	93.1%	4.2%	2.8%	0%	0%		
Frequency	67	3	2	0	0	1.10	0.381

Source: Research Data (2015)

Under information strength of existing security policies used by SACCOS, respondents were asked to indicate an approximate number of occurrences of security threats reported by their SACCOS in the last two years. Table 4.13 indicate that 55.6% reported that they have not been attacked by a computer viruses, 20.8% indicated that they have been affected by a computer viruses with an occurrence from 1 to 5 times, 18.1% said that they have been affected by a computer viruses from 6 to 10 times, 5.6% indicated that they have been affected by a computer viruses from 11 to 14 times and no SACCOS reported a computer viruses greater than 14 times. Computer viruses had a mean of 2.19 and a standard deviation of 0.929.

The study established that institutions have faced the following security breaches: computer viruses, hacking and unauthorized access to/use of data, the study thus confirms the findings by (Medlin et al., 2008; Khalifa, 2013) who established that the most security threats within organizations are those of computer viruses, hacking, and unauthorized access to/use of data.
The results for hacking incident (external), show that 91.7% indicated that they have not been hacked externally. 8.3% have been hacked externally from 1 to 5 occurrences; from 6 to 10, 11 to 14 and greater than 14 occurrences have not been hacked externally. Hacking incident (external) mean is 1.08 and a standard deviation of 0.278. According to Harris and Patten (2014), business leaders are now taking data security concerns more seriously than ever, given the effects of information security breaches on business and consumers.

Computer viruses, Trojan horses, and worms have evolved, posing significant threats to individual and corporate computer systems. Under unauthorized access to/use of data (internal), 68.1% have not had their internal employees access or use data without authorization, 29.2% have had their internal employees access or use data without authorization from 1 to 5 times, 2.8 percent have had their internal employees access or use data without authorization from 6 to 10 times. Occurrences from 11 to 14 and greater than 14 have not recorded any violations of unauthorized access or use of data by their internal employees. Unauthorized access to or use of data internally had a mean of 1.35 and a standard deviation of 0.535.

When the respondents were asked about the theft of hardware and/or software, 77.8 percent reported that they had not recorded any theft, 20.8 percent had recorded theft from 1 to 5 occurrences, 1.4 percent recorded occurrence from 6 to 10 times, from 11 to 14 and greater than 14 times had not recorded any incidents in their last two years. A mean of 1.24 and a standard deviation of 0.535 were achieved.

Computer-based fraud results indicated that 61.1% respondents had not experienced Computer-based fraud, 36.1 percent had an occurrence from 1 to 5 times, 2.8% had recorded an occurrence from 6 to 10 times, and none had recorded Computer-based fraud occurrences from 11 to 14 and greater than 14 times. Computer-based fraud had a mean of 1.42 and a standard deviation of 0.550. Under human error, 36.1% of the respondents indicated that they had not recorded any incident. The same 36.1% was recorded 1 to 5 times. 20.8% reported occurrences from 6 to 10 times, 1.4% report an occurrence from11 to 14 and 5.6% reported an occurrence greater than 14 times. Human error had a mean of 2.04 and a standard deviation of 1.067. This indicates that human error is a critical type of breach to most SACCOS.

The study confirms the findings by (Loeber, 2004) who established that most institutions report 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% of small institutions reported being attempted targets of malware, as compared to 21% of medium institutions and 35% of large institutions.

The results of natural disaster had 68.1% of the respondents had not recorded any occurrences, 29.2% had reported the occurrence from 1 to 5 times, 2.8% had reported an occurrence from 6 to 10 times, and from 11 times or more had not reported any occurrences of natural disaster. A mean of 1.15 and standard deviation of 0.399 was obtained. Under damage by disgruntled employee, 93.1% reported no security threats occurrence, 4.2% reported an occurrence from 1 to 5 times, 2.8%, from 11 and more occurrences reported no security breach incident. A mean of 1.10 and standard deviation of 0.381 was obtained from damage by disgruntled employee.

The study concurs with the findings by (Heiser, 2004) who established that the growing frequency and sophistication of cyber-attacks had increased, a record 46% of respondents identified cyber security as the top concern, according to The Depository Trust and Clearing Corporation's. The cyber security ranking is nearly doubled compared to DTCC's Systemic Risk Barometer Study in March 2014 where 24% of respondents cited cyber security as the number one threat. Heightened concerns over cyber-attacks have led many market participants (73% of respondents) to increase their investment in technology to detect and prevent cyber threats. Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password cracking programs to figure out poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential e-mail, or initiate unauthorized e-mails or transactions.

The study sought to determine the severity of the worst breach of each type that SACCOS has experienced in the past two years. With N.A = Not Applicable, S.W.I = Some What Insignificant, S.W.S = Some What Significant and H.S = Highly Significant

4.3.2 Severity of the Worst Breach in the Last two Years

Table 4: Severity of the Worst Breach in the Last two Years

Type of Breach	N.A	S.W.I	S.W.S	H.S
Computer viruses	0%	55.7%	33.3%	11%
Hacking incident (external)	0%	45.7%	35.3%	9.0%
Unauthorized access to use of data (internal)	0%	37.4%	23.6%	39%
Theft of hardware software	0%	23.5%	24.5%	52%
Computer-based fraud	0%	9%	35.3%	45.7%
Human error	0%	17.3%	23.4%	59.3%
Natural disaster	0%	53.1%	37.3%	9.6%
Damage by disgruntled employee	0%	53.1%	33.3%	13.6%

Source: Research Data (2015)

From the findings 55.7% of the respondents stated that security breaches as a result of computer virus has been somewhat insignificant , 33.3% of the respondents stated it has been somewhat significant, while 11% of the respondents stated it has be highly significant. This implies that security breaches among SACCOS for the last two years as a result of computer virus have been somewhat insignificant. The findings also revealed that 45.7% of the respondents stated that security breaches as a result of hacking incident has been somewhat insignificant, 35.3% of the respondents stated it has been somewhat significant, while 9.0% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of hacking incident have been somewhat insignificant. The findings concur with Li et al., (2016) who indicated that information security breaches could result in a significant financial impact on organizational performance. As such, business leaders need to understand the extent to which breaches can affect their organization. Business leaders must define information security guidelines to protect a firm's technology assets against internal and external threats (Figg and Kam, 2011). The guidelines should include an impact analysis of a data security breach to understand the effects of the availability, integrity, and confidentiality (AIC) of sensitive information, given that AIC is the foundation of information security. Financial institutions are within the scope of privacy laws because they hold such information as individuals' bank account numbers and much more. Focusing on the technology opportunities, NIST (2010) suggested that de-identifying information reduces the risk of data loss or misuse. De-identification of data refers to eliminating the link to a specific person (Future of Privacy Forum, 2014).

In addition, 37.4 % of the respondents stated that security breaches as a result of unauthorized access has been somewhat insignificant, 23.6% of the respondents stated it has been somewhat significant while 39% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of unauthorized access have been somewhat insignificant. Furthermore, 23.5% of the respondents stated that security breaches as a result of theft of hardware or software has been somewhat insignificant, 24.5% of the respondents stated it has been somewhat significant, while 52% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of theft of hardware or software has been highly insignificant.

The findings also revealed that 9.0 % of the respondents stated that security breaches as a result of computer-based fraud has been somewhat insignificant, 35.3% of the respondents stated it has been somewhat significant while 45.7 % of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of computer-based fraud have been highly significant.

In addition, 17.3% of the respondents stated that security breaches as a result of human error has been somewhat insignificant, 23.4% of the respondents stated it has been somewhat significant, while59.3% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of human error have been highly significant. The findings also revealed that 53.1% of the respondents stated that security breaches as a result of natural disaster has been somewhat insignificant, 37.3% of the respondents stated it has been somewhat significant, while 9.6% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of natural disaster have been somewhat insignificant.

Finally the findings revealed that 53.1% of the respondents stated that security breaches as a result of damage by disgruntled employee has been somewhat insignificant, 33.3% of the respondents stated it has been somewhat significant while 13.6% of the respondents stated it has been highly significant. This implies that security breaches among SACCOS for the last two years as a result of damage by disgruntled employee have been somewhat insignificant.

Many break-ins or insider misuses of information occur due to poor security programs. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by the institution. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper setup of available security-related tools. An institution needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep up to date on the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor Web sites contain much of this information.

5. Conclusion

Hacking incident, natural disaster, and damage by disgruntled employee have been somewhat insignificant.The study further concluded that security incidents and breaches are under reported. Given the prevalence of external hacking incidents the findings on human error, unauthorized access to use of data (internal), theft of hardware and software and computer-based fraud results was highly significant. This indicates that many break-ins or insider misuses of information occur due to poor security programs. Most of the employees knew about the use of security measure in

place when under a deadline to complete an assignment within the SACCOS.

6. Recommendations

From the conclusion the study concluded that SACCOS need to reinforce training of its employees and strengthen their policies to achieve enhance information security. To ensure the security of information systems and data, financial institutions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Institutions should consider the various measures available to support and enhance information security programs. The study concluded that security breaches among SACCOS for the last two years.

References

[1] Amancei, S. (2011) *Software Engineering Conference* (APSEC, 2013 20th Asia-Pacific (1). IEEE, Univ. of Luxembourg.

[2] 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-Mar 07-2007.pdf

[3] 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.

[4] CIO East Africa (2017) East Africa: Data Security – Safeguarding Your Business Network from Cyber Crime Retrieved from http://allafrica.com /stories/201711070967.html

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

[6] Figg, E. &Kam, V. (2011). Current Directions in IS Security Research: Towards Socio-organizational Perspectives, *Information Systems Journal* (11),127–153.

[7] Fihlani, P. (2017). Millions caught in South Africa's 'worst data breach'. BBC News. Retrieved from http://www.bbc.com/news/world-africa-41696703 G. USA: Idea Group Publishing, 1-8.

[8] Fulford, J. (2005). An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management (23)*, 139–154

[9] Greene, S. (2006). Security Policies and Procedures: *Principles and Practices, Upper Saddle River, NJ:* Pearson Education, Inc.

[10] Hagen, M., Albrechten, E., &Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

[11] Heikkila, F. (2009). *An analysis of the impact of information security policies on computer security breach incidents in law firms* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3380050)

[12] Humphreys, E. (2007).Implementing the ISO/IEC 27001: *Information Security Management System Standard,* Boston, M.A: Artech House

[13] ICA Annual Report (2016). *The 2016 International Summit of Co-operatives*. Retrieved from https://www.ica.coop/sites/ default/files/ publication-files/ enannual- report 2016final- 681195095.pdf

[14] Johnson, M. (2008). *Information risk of inadvertent disclosure*: An Analysis of File Richardson, R. CSI Computer Crime & Security Survey. Computer Security Institute.

[15] Kaarst-Brown, F. (2005) Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.

[16] Kenya Cyber Security Report (2016). Achieving Cyber Security Resilience: *Enhancing Visibility and Increasing Awareness.* Retrieved fromhttp://www.serianu.com/downloads/KenyaSecurity Report2016.pdf

[17] Khalifa, N. (2013). *Information Technology Capabilities in Enabling Electronic Banking*: Case Study of a Bank in a Developing Country. Journal of Electronic Banking Systems, 2013: 1-28

[18] Lin, P. (2006). *System security threats and controls*. The CPA Journal, 76(7), 58-66.

[19] Mangal, N. (2013) *Representing and Configuring Security Variability in Software Product Lines''*, Proceedings of the 10th International ACM SIGSOFT Conference on Quality of Software Architectures, pp: 1-10, ACM New York, NY, USA

[20] Medlin, D., Cazier, A., &Foulk, P. (2008). *Analyzing the vulnerability of U.S. hospitals to social engineering attacks*: How many of your employees would share their password? International Journal of Information Security & Privacy, 2(3), 71-83.

[21] Moga, M., Nor, M. &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

[22] Nassiuma D. (2000). Survey Sampling: Theory and Methods. University of Nairobi Press, Nairobi.

[23] Nation Newspapers (2014, September). *FBI seeks Kenya's help to arrest bank fraud suspects*. Retrieved from http://www.nation.co.ke/news/FBI-Kenya-arrest-bank-fraud-suspects/1056-2440408w5s2baz/index.html

[24] Rastogi, R., & Von Solms, R. (2006). *Information Security Governance a Redefinition. IFIP International Federation for Information Processing,* 1(93)

[25] Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology, 23*(3), 185-202.

[26] Siponen, M. (2000) Employees'adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

[27] Wallace, A., Creese, S., & Goldsmith, M. (2011). *Insider attacks in cloud computing*. 2011 IEEE International Conference on Trust, Security and

Privacy in Computing and Communication (TrustCom), 857–863. Liverpool, England: IEEE
[28] Whitman, M., &Mattord, H. (2013). *Management of Information Security* (4th edition) Boston, MA: Cengage Learning
[29] Wiant, R. (2005). A lesson in risk management. Insurance Networking News, 16(5), 24-26
[30] Wu, Y. &Rocheleau, E., (2001). Information security policy – what do international information security standards say? Computers & Security, 21(5), 402-409..
[31] Yaokumah, C. (2014) *The 10 deadly sins of information security management*. Computers & Security, 23(5), 371-376
[32] Yukl, J., (2006). Information systems security policies: A *contextual perspective. Computers & Security, 24*(3), 246-260