UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

CYBER SECURITY READINESS FOR MOBILE BANKING AMONG DT SACCOS IN NAIROBI COUNTY

JAVAN SYDNEY MATANDA

P54/37837/2019

RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT OF THE UNIVERSITY OF NAIROBI

NOVEMBER 2020

DECLARATION

I declare that this is my original work and has not been presented for a Master's Degree in any other University.

Signature  **……..** **Date**27/8/2021**……**

Javan Sydney Matanda

This research project has been submitted for examination with my approval as the University Supervisor.

Signature  **……..** **Date**27/8/2021**……**

Professor Agnes N. Wausi

ACKNOWLEDGEMENT

First and foremost I am extremely grateful to Almighty God for granting me health, energy and wisdom to carry out the master's studies. I'm as well grateful to my supervisor, Prof. Agnes Wausi for her invaluable guidance and advice, continuous support, and patience during my Masters study. I would also like to recognize Dr Bright (Strathmore University), whose insight and knowledge into the subject matter steered me through this research. Their immense knowledge and plentiful experience have encouraged me in all the time of my academic research and daily life. I would also like to thank Professor R. Oboko and Professor E. Opiyo for their technical support on my study. I would also wish to extend my gratitude and appreciation to all correspondents in the DT SACCO industry who participated in the research study. I wish to also acknowledge the University of Nairobi School of Computing and Informatics for approving and supporting my Research study. Finally, I would like to express my gratitude to my wife Elvin and my children Alvin and Aaliyah, without their tremendous understanding and encouragement in the past few years, it would be impossible for me to complete my study you have been amazing, and I will now clear all the learning materials off the study table and drawers as I promised!

ABSTRACT

The mobile Banking technology among the DT SACCOs has rapidly grown resulting from the digital transformation among the financial sectors. The technology is based on electronic banking where mobile can be transacted through mobile devices like mobile phones. The SACCOs ventured into electronic banking to meet the demanding and competitive banking markets (Salehi & Alipour, 2010).

There has been an alarming rise in the cybersecurity attacks within the financial industry that includes banks, microfinances, and SACCOs. These attacks have led to financial and other forms of losses like corruption or destruction of data, unauthorized access to confidential information, compromised system and applications and opportunity costs, including disruption in delivery of services (Wechuli, Wabwoba & Waska, 2017). According to GSMA mobile money report 2019, and Serianu report 2019/20 financial institutions have lost $1.7 billion via cybersecurity over mobile money hence need for address.

This research study is intended among other objectives to develop a cybersecurity blue print on Mobile Money Cybersecurity Readiness among SACCOs in Nairobi County by identifying a more suitable roadmap to implement the framework in the SACCO.

The study engaged a mixed type of methods in which a quantitative research strategy with a descriptive research design was used to gather data concerning to the status of the situation at the current state which is relating to topic being researched. At first, operationalization of the Linkert scales was done. A descriptive analysis was carried out, correlation and factor analysis was done followed by multiple regression analysis to the Linkert scales.

Based on the results, descriptive analysis demonstrated a perception that concerns the current cybersecurity mobile money readiness among the DT SACCO. From the correlation analysis there is a strong positive correlation and positive significant between the SACCO Governance Support and Contribution, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity Requirements and Proactive Mobile Money Monitoring & Audit were recognized as being the critical strategies influencing Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs in Nairobi City County in Kenya.

The study focused on collecting cybersecurity data from SACCOs which are financial institution and they regard such information as highly confidential and possess challenges obtaining it. The study was also conducted during the COVID 19 pandemic.

The study is of value as it addresses the gap where previous cybersecurity studies never prioritized mobile money. It also gives a Blue Print which guides the DT SACCOs to address the losses and create resilience for managing cybersecurity mobile banking readiness.

This research study concludes by giving a cybersecurity blue print on mobile money cybersecurity readiness among DT SACCOs and also insists the critical focus on the Proactive Mobile Money Monitoring & Audit strategy. The guidelines in the blue print are as well recommended to be adopted by other DT SACCOs of nature outside the study area.

Key Words: Cybersecurity, SACCO, Mobile Banking, Readiness, Blue Print, Adequate cybersecurity.

Table of Contents

Table of Figures

Table of Tables

Table of Abbreviations

Abbreviation	Word / Meaning
CBK	Central Bank of Kenya
CIA	Confidentiality, Integrity, Availability
CMMI	Capability Maturity Model Integration
COVID 19	Corona Virus Disease
CSx	Cybersecurity Fundamental Certificate
DT	Deposit Taking
FOSA	Front Office Services Activities
GSMA	Global System for Mobile Communications
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
IS	Information systems
ISACA	Information Systems Audit and Control Association
ISMS	Information security management systems
ISO	International Organization for Standardization
IT	Information technology
KNBS	Kenya National Bureau of Statistics
MFS	Mobile Financial Services
M-Pesa	M for mobile, pesa is Swahili for money
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	Operational Technology
PECB	Professional Evaluation and Certification Board
PIN	Personal Identification Number
PSP	Payment Service Providers
SACCO	Savings and Credit Cooperatives
SASRA	SACCO Regulatory Authority
SMS	Short Messaging Service
USD	United States Dollar

CHAPTER ONE

1.0. Background

There has been rapid technology transformation in the financial sector ranging from banking, insurance, microfinances and SACCOs. This is evidenced by innovation of electronic finance, money, insurance, exchange, brokering and electronic supervision. Electronic banking took effect deeply in distribution of channel services in finance initiated by technological advancement and demanding competitive banking markets (Salehi & Alipour, 2010). It has been noted that Customary Banking or traditional/branch banking has progressively been interchanged by electronic banking (Nkonge, 2018). According to statistics in CBK Annual Report 2019 electronic banking in Kenya grew to 75% a 37% increase compared to previous years. The tremendous growth has yielded the financial sector more so banking to adopt the changes. As the invention kept growing the invention of mobile financial services (MFS)-also called mobile money revolutionized financial infrastructure offering individuals opportunities to save, spend and transfer money by use of short messaging service (SMS) without formal bank account (Hove & Dubus, 2019) The increase in M-PESA, Kenya's largest has been remarkable success which keeps an eye of interest to researchers from various fields (Jack, Ray & Suri, 2013). M-PESA is a text message-based payments system that allows its users to receive, send, deposit, withdraw and save money as well as pay for services and goods using SMS text messages that are PIN-secure

1.1.1. SACCO BUSINESS

Savings and Credit Cooperative Society (SACCO) is a voluntary financial institution owned and controlled by its members and operated to drive provision of credit at low-interest charges, supporting savings and other non-financial services to its members (Waweru, 2011). In Kenya, SACCO are among the largest financial institutions fulfilling the needs of all people from different background (FAO, 2018). In 1908, Lumbwa cooperative was first SACCO to be formed by European famers to support agricultural activities and products which took economies of scale (Ministry of industry, trade, and Cooperatives, 2014). More than seven thousand had been registered by 1999 and due to this rapid growth need, a SACCO Societies' Act was legislated in 2008 to cover way for dynamic implementation of prudential standards for SACCOs with front office services activities (FOSAs). The enactment resulted to the SACCO Regulatory Authority (SASRA) the body charged with the responsibility of regulating deposit taking SACCOs. Most of these SACCOs are now depending on Information Communication Technology ICT to drive

business and by focusing on customer satisfaction and competitiveness whose metrics are convenience, service speed delivery, efficiency with cost-effectiveness (Cumby, 2018).

1.1.2. Mobile money

Mobile money to some extend is associated with mobile banking where customers access a bank account via a mobile phone; sometimes, they are able to initiate transactions while mobile money is a service in which the mobile phone is used to access financial services. According to World Bank Article Volume 33, issue 2, August 2018, mobile money is among the recent innovation which offers financial transaction services via mobile phones including the unbanked global poor. This mobile money technology originated from telecommunication industry which has exponentially grown since its first invention and launch in Kenya in 2007 by Safaricom (Wadada R., 2019). It is the most popular and successful mobile money in the world (Morawczynski, 2012).

1.1.3. Cybersecurity

There has been a varied range definition of cybersecurity by different authors. For instance Kaspersky define cybersecurity as the practice for defending computers, servers, mobile devices electronic systems, networks and data from malicious attacks. Cisco Incorporation define it as practices of protecting systems, networks and programs from digital attacks. According to Huawei it is the information technology IT security are techniques of protecting computers, networks programs and data from unauthorized access or attacks that are aimed for exploitation. In broad research concerning cybersecurity there are clear results of confidentiality, integrity and Availability of digital resources. For the purpose of this proposal, Cybersecurity is the collective application of strategies, security measures, threats administration tactics, training, paramount practices, assurance and expertise that can be used to guard the mobile money/banking system, SACCO, members/customers and all related assets (International Communication Union, 2004).

Economic Impact of Cybercrime – No Slowing Down, estimates that the cost of cybercrime in 2018 worldwide was USD 600 billion.4. These costs can be both direct and indirect. The estimated cost of cybercrime in 2018 in Kenya which has the world's largest mobile money was reported as $295 million, $88.5 million were direct cost and $206.5 million indirect as cited by GSMA mobile money 2019.

1.1.0. Problem statement

There has been an alarming rise in the cybersecurity attacks within the financial industry that includes banks, microfinances, and SACCOs. These attacks have led to financial and other forms of losses like corruption or destruction of data, unauthorized access to confidential information, compromised system and applications and opportunity costs, including disruption in delivery of services (Wechuli, Wabwoba & Wasike, 2017). When financial services become progressively more digitized, so is the volume of sensitive digital data grows exponentially with it. Studies have shown that among the financial categories, banks and microfinances have mitigated these risks by mainstream cybersecurity frameworks developed and implemented successfully (DFS Guideline Note No.37, 2019). As cited by GSMA Mobile money Report 2019, 1.7 billion people in the world still unbanked hence critical that mobile money is left as the reliable lane to financial access, beyond that services continue to expand and innovate (The Global Findex Report, 2017). The mobile money is among the technologies that are key to achieving the World Bank goal of Universal Financial Access by 2020. In Kenya, though SACCOs have played critical significance in uplifting lives of people in the community through financial inclusion providing frequent services which cannot be found elsewhere. For instance in rural areas many farmers depend on SACCO credit and payment services (SASRA Report 2017). According to the SACCO Cybersecurity Report 2018 Demystifying Cybersecurity for SACCOs by Serianu, 95% of organizations within Africa operate below the Cybersecurity poverty line and with the SACCOs institutions included as having a heavy economic impact to the Kenyan economy will need proper risk management as they innovate mobile money technologies.

Despite the government of Kenya formulating the SACCO Society Regulatory Authority (SASRA) in 2009 to secure the SACCOs and their members by formulating guidelines on risk management practices, SACCOs focus on Compliance which is only a sole requirement which they don't fully measure, and fail to focus on the cybersecurity framework for mobile money that is taking a huge economic drift in the portfolio.

1.1.1 Justification of study

The research study aims to provide a guide to many DT SACCOs generally in having good Mobile banking cybersecurity to safeguard the members' funds. This study is very important to scholars

since previous studies that have been conducted focused on the general Cybersecurity studies and cybersecurity cultures in organizations and other well recognized financial institution like banks and microfinances. There have also been attempts by scholars both locally and globally to study the cybersecurity mobile money for the Banks. This has made cybersecurity mobile banking among the SACCOs a grey area to be researched.

SACCOs are the economic and financial cushion to majority of the population in Kenya. Based on that focus it is important that even as they keep growing technologically and economically, Cybersecurity deficiency among other related issues should not reap them off their resources through mobile money. According to Kenya Government Vision 2030, it is envisaged that co-operatives shall provide a 25% economic share to impact the country in major projects like urban housing, education among others. The study is therefore significant in all perspectives

1.2.0. Objectives

1.2.1. Main objectives

1. Develop a cybersecurity blue print on Mobile Money Cybersecurity Readiness among SACCOs in Nairobi County by identifying a more suitable roadmap to implement the framework in the SACCO

1.2.2. Specific objectives

2. Identify and review mobile money frameworks in place.
3. Identify Adequate Mobile Money Cybersecurity Blue Print for the SACCOs
4. Evaluate key factors that demonstrate cybersecurity readiness in SACCOs.

1.3.0. Research Questions

i. What are the stages for Mobile Money Cybersecurity Readiness in your SACCO?
ii. Does the current Monitoring and Audit of Cybersecurity in place contribute to Mobile Money Cybersecurity Readiness in your SACCO?
iii. Which are the current Cybersecurity Frameworks being implemented for Mobile Money Cybersecurity Readiness in your SACCO?
iv. Are the current staff skills, training and certifications in cybersecurity enough to Mobile Money Cybersecurity Readiness in your SACCO?

v. Does the ICT Service Vendor Management affect Mobile Money Cybersecurity Readiness in your SACCO?
vi. Have your SACCO designated Mobile Money Cybersecurity Readiness assessment tools?
vii. How is the SACCO top management prepared for the Mobile Money Cybersecurity Readiness?

1.4.0. Limitations of the research

i. COVID 19 pandemic which bears challenges of correspondence.
ii. Some data and information required by the researcher are confidential and may not be shared.
iii. There are cost constraints proving to be high for the research and related requirements of study such as questionnaire preparation.

1.4.0. Addressing the research limitation

i. The research will be carried out in compliance with the COVID Healthcare Guidelines and digital online forms will be used.
ii. The study questionnaire forms will bear no identity (Name) of the respondents.
iii. There will be means of soft copy questionnaire to work with the available budget.

1.5.0. Basic assumptions in the study

i. That the selected SACCOs uses the mobile money services and will provide all data that is required.
ii. That the respondent answered truthfully and correctly all the questions that had been asked.

1.6.0. Definitions of terms

Information systems IS- the combination of the technology, processes, people and data working in synchronous model to deliver set objectives for an organization.

Internet of Things (IoT) - A collection of both the electronic devices capability and can be linked with the internet to give human interaction interface.

CHAPTER TWO

LITERATURE REVIEW AND RESEARCH FRAMEWORK

2.0. Introduction

The chapter presents what other researchers have already written with regard to how the use of mobile money influences the savings patterns of individuals, with an aim of locating this research within the existing literature context with the intention of understanding the research problem and identifying the existing research gaps.

With the increased cases of cyber-attacks targeting mobile money services in payment service providers like SACCOs, the available material for literature for cybersecurity sponsors improved focus on the safe and secure adoption of risk-free adoption of mobile money technology. Developing the most effective cybersecurity framework empowers the organization to manage and safeguards the adoption, implementation and use of mobile money. Most challenges facing the use and the adoption of mobile money services like complete registration of the required document were being deliberated during the implementation and adoption period by vendors/operator and never kept the consistencies practice and culture by the organization (Nyaga & Ogollah, 2016).

2.1.1. Mobile money and Cybersecurity Over view

Mobile money services continue be the most prevailing aspect which continues to raise growth across the developing countries and the many Payment Service Providers (PSP) organization in Kenya. Mobile money has been defined differently by authors, for instance GSMA defines it as a service which mobile phone is used to access financial services (Wadada, 2019). Mobile money is the smorgasbord of innovative and cost-effective financial services accessible via mobile phone (Adaba & Ayoung, 2017). The later definition is preferred since it covers the broader aspect of innovation that is founded on the technology as a platform. This set the precedence for connecting the risks associated with its adoption linking cybersecurity as the major one.

Cybersecurity has been widely used and differently defined in the broader context ranging from the academic to industrial perspectives. The most preferred definitions are the ones that incorporates the multidimensionality of cybersecurity enhances innovations and specific progresses that reinforces the mostly technical perspective of Cybersecurity and segregating discipline that work collaboratively to mitigate complex cybersecurity challenges. Cybersecurity is the association and collection of means, processes, and structures for protecting cyberspace and

cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Craigen et al., 2014)." The cybersecurity has always been a subject at both industrial and academic level since its evolution. In the literature all the authors for different definitions have been scrutinized and brief critics presented and analyzed the definitions. In all the definitions the most common themes featured: - strategies, processes and methods, technology solutions, human engagements, events and referent objects (of security). The themes have demonstrated interdisciplinary nature and aided important context for a modern definition of cybersecurity (Adaba & Ayoung, 2017; Craigen et al., 2014).

All the definition remain enough and substantive to be understood in the general environment. The deeper understanding and its practicality that comes with the technology in mobile money will help the industry key players in keeping organizational resources and technology assets secure both information and non-information with the industry scope beyond just the technical understanding(Gong & Philbin, 2016).

Cybersecurity has been used interchangeably with Information security. They have not been able to differentiate the terms. It is therefore important to draw a distinction between the two terms as the focus is directed to Mobile money and have clear knowledge on their relationship. Based on the International standard of information security, ISO/IEC 27000(2016), the information security is protection of information against unauthorized access (availability), unauthorized disclosure and unauthorized modification.

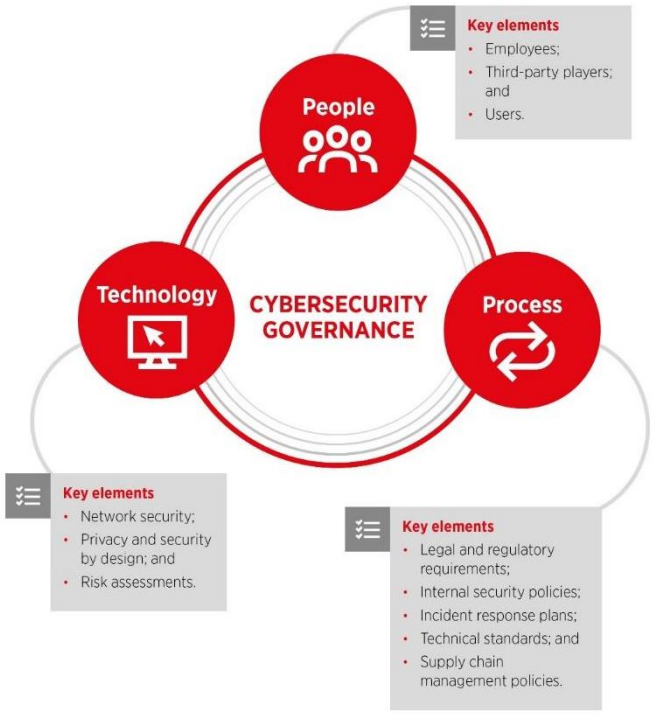
The Kenya cybersecurity strategy (2014) has also defined cybersecurity as protection of ICT infrastructure, information and services from the unauthorized access, destruction or alteration.

The Garner 2019 recognizes cybersecurity as being a consortium of personnel, policies, processes and technologies applied within an organization to safeguard the cyber assets. The issue of business has been clearly brought out hence integrating the cybersecurity and its significance in the business charging the business leaders responsibility of balancing required resources with required usability and risk. There has been clarity on the information security and cybersecurity and how they relate. The components of cybersecurity have been clearly categorized as Information technology (IT) Security, Information Security, Internet of Things (IoT) Security and Operational Technology-OT security (*Gartner*, 2020.)

The cybersecurity is so broader and multidimensional issue which is deduced differently across different sectors. Rationally, for mobile money industry, the general understating will be he safeguarding the network-related structures (technical infrastructure, Confidentiality, Integrity, availability-CIA Triad, procedures workflows and devices (mobile phones, laptops, etc.) and the software and data they contain. The practice have been narrowed down to hold only practices which support the secure operations and activities of mobile money and the members and other customers using the mobile money services in a SACCO.

Below is a generalized view of both GSMA and Gartner concept of Cybersecurity components.

Figure 1; Components of the cybersecurity



Source: GSMA.com ("Cybersecurity," 2019)

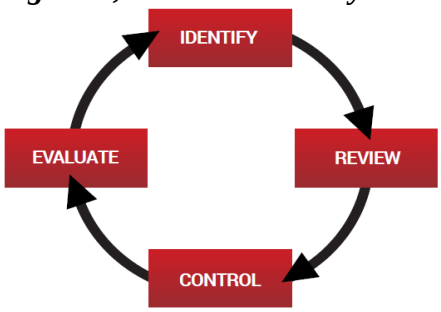
2.2.0. Theoretical Framework

Knowledge around the mobile money cybersecurity has been so widely described and theories developed in understanding the cases. The theories covers their biased areas of focus and can be relied upon at times of specific address and events.

2.2.1. ISO 27001 Control framework.

The international standards which has categorized and set the provisions for Information security management systems-ISMS. The framework has set the arrangements and industrial bets-practice specification approaches that support the implementation, certification and compliance with the cybersecurity components ranging from people, technology and processes (PECB, n.d.). The theory maps out the key step to information framework and aids in identifying the risks and controls to be performed. The framework contains the cyclic view of evaluate, identify, review and control. The emphasis is on the governance of Information Technology security (Calder & Watkins, 2012).

Figure 2; ISO revolution cycle

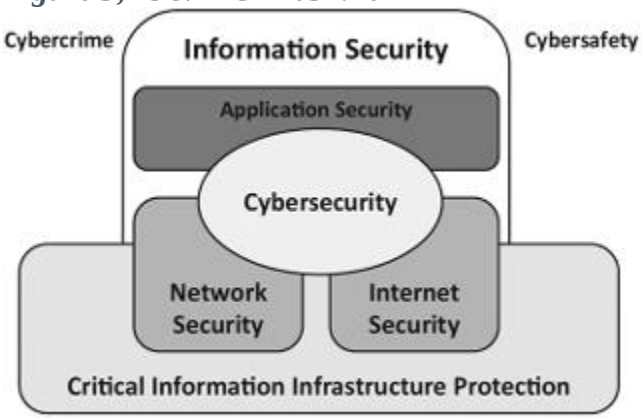


Source: (PECB, n.d.)

2.2.2. ISO/IEC 27032:2012 Framework

The international standards for organizations created this standards together with the organization for standardization and the international electro technical Commission in 2012. Cybersecurity has been multifaceted as confidentiality, integrity and availability (CIA) of information that is restricted in cyberspace. The sophistication of cyberattacks needed advanced approach and the framework was developed for the provision of guidance for the advanced stage of cybersecurity by pointing unique aspect of the exact activity and its reliance on the other domains of security. Its span for security practices is across stakeholders in the cyberspace (14:00-17:00, n.d.).

Figure 3; ISO/IEC 27032:2012



Source; cyberspace (14:00-17:00, n.d.).

2.2.3. ISACA CSx Cybersecurity Fun Theory

The ISACA history for cybersecurity is widely known and appreciated in the streamlining of cybersecurity and operations of technology in the SACCO industry. The theory presumes to define cybersecurity as an industrial-based risk that requires specific mitigation i.e. SACCO as a financial industry. The fun theory proposes the development of unique cybersecurity model to counter the risks by offering training for cybersecurity fundamentals and certification of the same. The modelled training marks the entry-level professional certificate for cybersecurity. It is also aligned with the national Institute of Standards and Technology-NIST and National Initiative for Cybersecurity Education-NICE. The theory has been widely utilized in cybersecurity research, though the theory has not featured so much in scholarly research it dominates in the industry grassroots. It has been in existence longer than other frameworks.

2.3.0. Review of Empirical studies.

The cybersecurity study conducted by ISASA/CMMI globally in 2018 and Serianu 2020 report on African cybersecurity focused mostly on mobile money cybersecurity. The studies demonstrated the impact of the cyberattacks targeting the mobile money technology that is escalated by the financial motivations. The studies showed how the stakeholders all over the world have kept researching, policymakers, regulators and industry players still keep on grappling with on the ways to counter the emerging mobile money cyberattacks. This has evidently proved that significant gap existed between the normal cybersecurity and the mobile money cybersecurity. In reference to

ISACA/CMMI global cybersecurity 2018 study, the statistics on the studied organization related to cyberattacks represented 4,815 organizations that were surveyed, 32% showed mobile money cybersecurity gaps. In the Africa Cybersecurity report 2019/2020 showed that there was a total of 51,903,286 cyber threats reported with 40,893,141 being the malware attack and 6,109,184 for application attacks. These most affected areas of the attack base are directly or indirectly associated with mobile money and its infrastructure (Kitime, 2018). The literature is presented in much more of the report and gives less guidelines on what to adopt to achieve the solution. It is therefore critical that the revision be submitted since in its current condition it does not give assurance for acceptance.

Locally, research for instance C. Moturi & G Ogoti (2020), describes the tremendous growth of innovative mobile money services in lending. The author also reiterates that while there are positive results emanating from technology-enabled financial inclusion, so are the risks and hence calls to action the need to strengthen the ability of technology risk management. There are as well defined proposition strategies and practices that can safeguard the financial technology ecosystem (Moturi & Ogoti, 2020). This literature has been accepted as is and applauded.

A varied number of research like (Kitime, 2018); (Harris et al., 2012); ("Cybersecurity," 2019), (Gong & Philbin, 2016) and (Moturi & Ogoti, 2020) among others have recognized the cybersecurity framework for mobile money as an operational and most effective elucidation to mitigate risky mobile money cybersecurity.

From the above reviews, authors have assessed good and reliable coverage of cybersecurity maters and concluded with great recommendations, there have been also great magazines, journals and reports and analyses on the cybersecurity however the area of Mobile Money cybersecurity among the DT SACCOs seemed fallow.

2.3.1 Understanding of the Cybersecurity Strategies Relating to Mobile Money Cybersecurity in DT SACCOs

In reference to the Information Security and Cybersecurity Frameworks discussed above and the forgoing discussion on Mobile Money Cybersecurity Readiness critical strategies were noted that can impact adequate Cybersecurity Mobile Money Readiness among the DT SACCOs. In

conjunction with the generalized view of both GSMA and Gartner concept of Cybersecurity components (GSMA, 2019), the study recognized Governance Support and contributions to Cybersecurity, Service Level Agreement & Policy management, Mobile Money Cybersecurity Readiness.

According to Calder (Calder & Watkins 2021) in the ISO 2700 Control framework the study also identified Cybersecurity Skills, training and awareness programs, and Regulatory and Legal Compliance requirements strategies as the best industry practices that combine several components like people, technology and processes. The framework gives a revolution cycle that begins from Identity, review, control and finally evaluate the components involved in the Cybersecurity. The framework is also considered critical in most organizations focusing on the Information Security Management Systems.

ISO/IEC 27032:2012 Framework being an international standard insist on confidentiality, integrity and availability –CIA It is mostly used in many enterprises globally in the domains of security. The framework bases on technology security and partly legal aspect that spans to cybercrime prevention-Cyber safety.

ISACA CSx Cybercrime Fun Theory demonstrated a streamlined cybersecurity and operations of safe technologies in the SACCO industry. The theory combines the integrated frameworks customized for SACCO industry model. The Frameworks integrated here include the NIST and the NICE. The theory is so much closely related to the industrial scenarios tested and affirmed the variables.

The reviewed theories and frameworks presented Governance Support and contributions to Cybersecurity, Service Level Agreement & Policy management, Cybersecurity Skills, training and awareness programs, and Regulatory and Legal Compliance requirements and Proactive Mobile money monitoring and Audit strategies to be adopted on the Conceptual framework of the study. They are notable selected due to their direct or indirect effect to the adequate Mobile Money Cybersecurity Readiness in DT SACCOs especially that majority of them are already operating.

SACCO Governance Support and contributions is the critical strategy to achieve an adequate Mobile Money Cybersecurity readiness in among the DT SACCOs. This is because SACCO's decisions are based on the governance structure – the leadership structure mostly at the top

involving the board, members delegation and other stakeholders. They are important in making decisions like approval of budgets and approval of necessary structures. The structures are key in achieving the adequate mobile money Cybersecurity readiness. The governance can as well support the cybersecurity via the top management contributing and leading by examples to achieve the adequate mobile money Cybersecurity readiness the SACCO (Zainudin, 2017).

Service Level Agreement & Policy management is the combination of how the innovation or technology vendors have a guideline that define the expected service level. This has the metrics that have been laid out against the service to be measured. The aspects of remedies in case of the uncertain incident and penalties to a SACCO and also the Policy management are key guideline pointing cybersecurity and IT operations in a safe environment (ISACA CSx: 2018). This is very important strategy that provides how both the staff and vendors conduct themselves in support of adequate mobile money cybersecurity readiness in any organization by way of compliance to the policy, compliance with the documented guidelines in both the Service Level Agreement and Policy.

Cybersecurity Skills, training and awareness programs are very important as it focuses on the people perspective who are responsible for ensuring Mobile money Cybersecurity Readiness. The skills developed and acquired for cybersecurity prepares the personnel to handle the cyber-related matters both technically and administratively. The trainings which can be organized both internally and externally equips the organization the required. An organization also needs to plan and run awareness programs which brings knowledge to all stakeholders in ensuring they are well prepared with the any past, prevailing and future cybersecurity issues (ISO 27001:2018).

Regulatory and Legal Compliance requirements are key for observation in any business entity operating in any state. The requirements in cybersecurity varies beginning from that of state laws, regulatory agencies, and specific industry law like those of GSMA, Payment Card Industry & Data Security Standards-PCIDSS. These set of regulatory requirements have been formulated to cub the emanating cybercrime and on the path to follow in case of any incidences. They are mostly viewed as external support from the respective legal agencies, government initiative and specific industry and professional bodies. These requirements directs the DT SACCO on the basic guidelines to observe and implement to be legally safe-guarded. The guidelines directs the way DT SACCO should disclose their cybersecurity breaches.

Proactive Mobile Money Monitoring and Audit being the most strategy for monitoring and controlling cybersecurity in any organization. It is termed as the power to operational risk monitoring within any environment an organization can adopt and have. The monitoring is across the whole organization components ranging from people, processes, technologies, hardware and software (applications). Real-time monitoring using the automated technologies and audits where regular examinations are carried out in the well-defined methodologies like the assessment of the vulnerabilities within the applications and hardware (ISACA, 2018). This strategy is important as the attacks, attack signals, threats and other uncertainties. Having the practices in place by the management would ensure preventive measures in handling the shortcoming.

2.4.0. Conceptual framework

This section holds the conceptual framework which informed the study. The framework provided by ISACA was chosen for its ability to link business, academia and industry by means of research. The cybersecurity on mobile money and how they relate in technology and finance environment. The dependent variable was conveyed through mobile money cybersecurity in the SACCO. The conceptual framework later derived the research methodology.

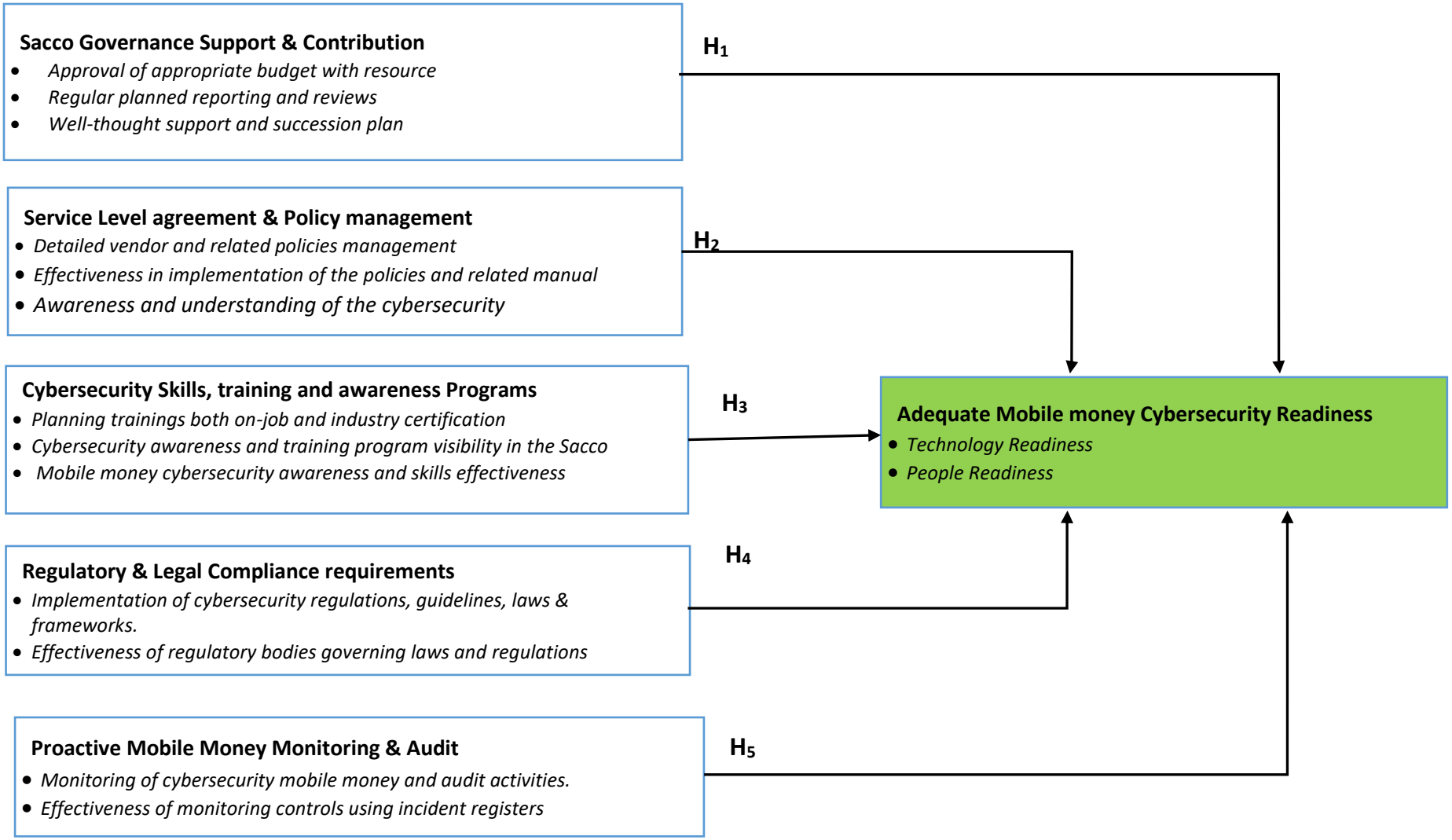


Figure 4 Source: Author, 2021

SACCO Governance Support & Contribution

SACCO Governance Support & Contributions is the most considered effective high level order group of representatives from the stakeholders like top management, members' representatives and other interested groups like regulator representatives and others. The governance consist of a structure having well defined functions in overseeing all the SACCO matters. It is cascaded down into special committees with each having roles. Such committees are like Supervisory Committee, Education Committee, Finance Committee, and Audit Committee among others. The construct has been considered in the Conceptual Framework since it is critical in the achieving the adequate Mobile Money Cybersecurity Readiness.

The change in the SACCO Governance Support and Contribution could has been considered as a dependent variable. Its change may lead to a change in the achievement of the adequate Mobile Money Cybersecurity readiness. The indicators for SACCO Governance Support and Contribution has also been based on the roles they are charged with. These are; Approval of appropriate budgets; regular review of the reports and creating a strategic succession plan. It directly relates to the adequate Mobile Money Cybersecurity readiness.

Service Level agreement & Policy management

The Service Level Agreement is the mutually agreed and binding agreement defining how mostly vendor as a service provider and the client the SACCO parties. The contracts are very key especially in achieving the adequate Mobile Money Cybersecurity Readiness. The partners who support SACCO in their innovation journey can directly or indirectly by exposing the vulnerable areas in which they are supporting. The rogue vendors themselves might be the threat as well. This construct has been considered as the second effective strategy whose effect is critical in the Conceptual Framework.

The Policy management deals with the set policy guidelines developed and updated and implemented in the SACCO. The Cybersecurity policy is the key policy to safeguard digital platform and related ICT resources. The policies are important and critical in this Framework as it directly affects the both project and operations relating to cybersecurity. The metrics to be considered here include; Detailed vendor and related policies management; Effectiveness in implementation of the policies and related manual; Awareness and understanding of the

cybersecurity. These makes the Service Level agreement & Policy management construct directly affect the Adequate Mobile Money Cybersecurity Readiness.

Cybersecurity Skills, training and awareness Programs

Cybersecurity Skills, training and awareness Programs is the construct that effectively support the preparedness in the skills required to handle the incidences, technical capability required to develop through training to manage cybersecurity. The awareness programs among the SACCOs promotes the preparation of how to respond to the trending and most disturbing cybersecurity matters. The construct is very important strategy and has been considered on the conceptual framework to highlight key indicators that have influence on the Adequate Mobile Money Cybersecurity Readiness. The key indicator to support this are; Planning trainings both on-job and industry certification; Cybersecurity awareness and training program visibility in the Sacco and Mobile money cybersecurity awareness and skills effectiveness.

Regulatory & Legal Compliance requirements

Regulatory & Legal Compliance requirements is a construct that has been considered in the conceptual framework to auger cybersecurity matters with legal and compliance aspect. This involves laws, standards and other regulation. The business environment under which the SACCO operations are dependent on the regulations from both the legal, business, technology and other related agencies like tax. The construct has been considered on the Conceptual framework to align how mobile money cybersecurity maters can be dealt from a legal perspective. Among the indicators for Regulatory & Legal Compliance requirements are: Implementation of cybersecurity regulations, guidelines, laws & frameworks; Effectiveness of regulatory bodies governing laws and regulations.

Proactive Mobile Money Monitoring & Audit

Proactive Mobile Money Monitoring & Audit has been considered and included in this conceptual framework as independent variable as it directly affect the Adequate Mobile Money Cybersecurity Readiness. Continuous monitoring and real-time detection of mobile money cybersecurity incidences keeps the SACCOs updated and ready to mitigate and prevent further incidences from happening. The Proactive Mobile Money Monitoring & Audit has been given a focus from the key

indicators that can affect the Adequate Mobile Money Cybersecurity Readiness. Among them are: Monitoring of cybersecurity mobile money and audit activities; Effectiveness of monitoring controls using incident registers.

Hypotheses of the Study

The study tested the following hypothesis: The hypothesis are also based on the way the variable construct have been used on the Conceptual Framework

H1 SACCO Governance Support and contribution on Mobile Money Cybersecurity program greatly contribute to Cybersecurity Readiness among the Deposit Taking SACCO in Nairobi City County in Kenya.

H2 Contracts with Technology Vendors and Service Level Agreement Management have a greatly support Mobile Money Cybersecurity Readiness among Deposit Taking SACCOs in Nairobi city county in Kenya.

H3 Mobile Money Cybersecurity Skills training increases Mobile Money cybersecurity Readiness for the Deposit Taking SACCOs in Nairobi City County in Kenya.

H4 SACCO's compliance to cybersecurity Legal, regulatory guidelines greatly contributes to Mobile Money Cybersecurity Readiness for Deposit Taking SACCOs in Nairobi City County in Kenya.

H5 Proactive Mobile Money Cybersecurity monitoring and audit greatly support and positively impact Mobile Money cybersecurity Readiness among Deposit Taking SACCO in Nairobi city County in Kenya.

Operationalization of the variables

Table 1; Operationalization of the variables

Variables		Indicators	Measures
Independent Variables	**SACCO Governance contribute to Cybersecurity resilience**	• *Approval of appropriate budget with resource* • *Regular planned reporting and reviews* • *Well-thought support and succession plan*	**1-5 Point Rating Scale**
	Service Level agreement management & Policy Management	• *Detailed vendor and related policies management* • *Effectiveness in implementation of the policies and related manuals* • *Awareness and understanding of the cybersecurity*	**1-5 Point Rating Scale**
	Cybersecurity Skills training improves knowledge & awareness	• *Planning trainings both on-job and industry certification* • *Cybersecurity awareness and training program visibility in the SACCO* • *Mobile money cybersecurity awareness and skills effectiveness*	**1-5 Point Rating Scale**
	Regulatory & Legal Compliance requirement	• *Implementation of cybersecurity regulations, guidelines, laws & frameworks.* • *Effectiveness of regulatory bodies governing laws ad regulations*	**1-5 Point Rating Scale**
	Proactive Mobile Money Monitoring & Audit	• *Monitoring of cybersecurity mobile money and audit activities.* • *Effectiveness of monitoring controls using incident registers.*	**1-5 Point Rating Scale**
Dependent Variable	**Adequate Mobile money Cybersecurity Readiness**	**Technology Readiness** • *Implemented mobile money cybersecurity devices and equipment.* • *Minimal mobile money cybersecurity incidences* • *Accurate automation of the SACCO Systems & operations*	**1-5 Point Rating Scale**
		People Readiness • *Staff trained with Mobile Money Cybersecurity skills.* • *Staff have knowledge on specific topics and contents* • *SACCO members trained and able to securely transact on mobile money.*	**1-5 Point Rating Scale**

CHAPTER THREE

RESEARCH METHODOLOGY

3.0. Introduction

The chapter views the research methods used for the study in order to address the objectives of the study and present the results from data obtained during the period of study. The subheading include; The Research Design, Target Population to be studied, Sample size and sampling techniques, Data collection instrument and procedures, Validity and reliability techniques and Ethical considerations.

3.1. Research Design

The research design is meant to provide an appropriate framework for a study. The proper research design choice and decision determines the relevance of the information for the research approach. This research design process comprises many organized decision (Jilcha, 2019). The study engaged a mixed type of methods in which a quantitative research strategy with a descriptive research design was used to gather data concerning to the status of the situation at the current state which is relating to topic being researched. These design was more preferred as the research initially intended to comprehensively describe status in their real picture during the period of study instead of influencing the study variable.

Descriptive research portrays and accurate profile of events, persons or situations hence offering the study a contour of described important features of occurrences of interest the digital google forms survey method was contained in collecting the primary data. The method is preferred as it was the only accepted and more secure method during the COVID 19 pandemic where physical meetings were impractical. A google form link which will contain the questionnaire as data collection tool will be send through the emails, what's App messaging and Short Messaging Services –SMS to the target organization or individuals and will be administered to the respondents by the help of contact person in the organization.

The limitation to this research methodology is that the results may take longer to be received as the population respondents may only respond to the questionnaire at their own convenient time which may push the datelines rather than earlier planned.

3.2.0. Target Population of the Study

Population refers to the complete set of individuals (events or subjects) that have similar characteristic in which the researcher is interested (Jilcha, 2019). The research populations involved in this study includes the active Deposit Taking SACCOs registered and licensed by SASRA in the Nairobi City County as at 31st December 2020. The SACCOs have been geographically distributed and the distance among them is uneven for instance they may be close to each other or far away. They may also be related as branches or not related in whatsoever manner. They differ from each other in terms of asset portfolios, membership rates and share capitals.

3.3.0. Sample Size and Sampling Procedure

Having reviewed different procedures and models to create sample size including Parton Distribution function and formula which also insist on normalization scheme and scale dependence on the size of the population, the study preferred to use Fisher formula that was suggested by Hossana-Chowdhury, (2011) and Zou (2012) since it is heterogeneous and gives a great view of the data that is less than ten thousands with a confidence interval of 95% in random strata. Below is the formula;

$$\boldsymbol{n = \frac{z^2 pq}{e^2}}$$

$n - Desired\ sample\ size\ n\ less\ than\ 10{,}000$

$z\ - Standard\ normal\ deviation\ at\ 1.96\ corresponding\ to\ 95\%\ confidence\ Interval$

p

$- Estimated\ proportion\ of\ target\ population\ (\ the\ personnel\ responsible\ for\ Sacco$

$$\boldsymbol{n = \frac{1.96^2 pq}{e^2}}$$

Among the 175 Deposit Taking SACCOs registered and licensed by SASRA as at 31st December, 2020 (SASRA, 2020) The study identified 44 active DT SACCOs is a about 25% of the total population. This was applied in picking respondents out of the selected areas of the Deposit-Taking-DT SACCOs who are believed to possess the critical data and information in line with the research problem. These will encompass of the respondents of both senior and junior personnel responsible for cybersecurity matters, ICT technical staff, ICT Head, a general user of ICT, customer care representative where complaints are logged will be selected in every

Deposit-Taking SACCO. This will be of great relevance in understanding the cybersecurity that is associated with utilization of mobile money and practices.

The table below illustrates. (Table 2)

Table 2; Total Number of Respondents in DT SACCOs

S/No.	Respondents for the study per DT SACCO	Representation
1	ICT Head	1
2	Senior personnel responsible for cybersecurity matters	1
3	Technical ICT Staff	1
4	General ICT Staff	1
5	Customer Care Staff	1
	Total number of respondents in selected DT SACCO 5*44	**220**

3.4.0. Data Collection Methods

3.4.1. Data sources

Primary data sources; these is the data that will be obtained directly from the original source of information. The research considers this the most reliable and will have more confidence level of decision-making with the trusted analysis that will expose direct instance with the occurrence of the events. These sources will be DT SACCO working environment (real-time transaction encounter, response to cyberattacks) and SACCO employees (interview & questionnaire).

Secondary data sources; desk review will be conducted for data collection from various secondary sources including but not limited to regulators, customers, competitors, vendors, national statistics reports (KNBS). As observed, this will be obtained from literature in regard to Cybersecurity of mobile money among DT SACCOs. Others will be reputable journals, books periodicals proceeding, magazine, newsletter, websites and other sources to be considered for desk review.

For this research the desk review was completed to the very end and polished. Both primary and secondary data will be used in the study as comprehensive cybersecurity for mobile money service aspects into smaller understandable interpretations.

3.5.0. Validity and Reliability

The content received from the sources were validated in the study to ascertain the extent which the received data with data collection tool is measured. The questionnaire was subjected to scrutiny by experienced researchers from the University of Nairobi and any other interested scholar for the content validity before it was dispatched to the field. There was reliability on the questionnaire that has been approved and that is appropriate for research. The questions in the questionnaire ensured consistency in the responses that were given. The contacts (email, mobile Phone numbers and SACCO emails) of the targeted respondents for the research was consolidated and the questionnaire was dispatched through the official researcher's email. The follow-up communications was followed later on the key contacts additionally via phone calls.

3.6.0. Data Analysis Methods

An accurate and objective check and analysis was done on the filled in questionnaire once collection of data and before coding and entering the data in SPSS software for analysis. This comprehensive check on the questionnaire ensured that any possible errors and omissions were noted. The analysis method of data was proposed to be the descriptive, inferential and regression statistics technique that considers quantitative data that were conducted for the research. The modal measurements, means, frequencies, standard deviations and percentages. The correlation and multiple regression analysis were considered in the inferential statistics.

3.7.0. Ethical Consideration

The researcher sought the approval from the management of the intended DT SACCO before collecting data. The researcher was as well registered as a data processor and sought legal consent as stipulated in the Data Privacy Act 2019 and complied as deemed due. The researcher bears responsibility of moral obligation to utilize the information shared for the intended study work. The declaration message will be accompanied with the digital questionnaire for the same assurance to the respondents of the use and confidentiality of their information. The participation is also voluntary and so the respondents' contrary opinion not to participate was respected at any time of research. They may as well respond from any geographical location of their choice.

3.8.0. Expected Contribution

The research aims at creating a comprehensive understanding and integrated cybersecurity readiness in mobile money technology. This will focus on solving the risks associated with the use of innovations alongside business and finance. The framework to bridge the industry practices and academia linking the stakeholders (regulators, fintechs, customers etc.) and business cycle. The main aim is focused on generating the solution as well to the rapid growing cyberattacks to SACCOs and any related business entity that may be having same or close business operation and processes.

CHAPTER FOUR

4.0 DATA ANALYSIS FINDINGS AND DISCUSSION OF THE FINDINGS

4.1 Introduction

The chapter presents areas of research data Analysis, the findings of the research and discussions on the research findings. The presentation of the findings is in alignment with the research methodology and research objectives in order to address research questions. The verdicts has results on demographic characteristics, descriptive analysis and inferential statistics. The research study was carried in the 44 identified DT SACCOs. Among the identified DT SACCOs identified an ICT head of department, one senior personnel responsible for cybersecurity matters, a technical staff and a general ICT staff and a customer care staff were asked to provide their responses and observation in line with the Cybersecurity readiness for mobile banking in their SACCOs.

4.2 Response Rate

The research study dispatched a total of 220 questionnaires out to the target DT SACCO. By the time of analysis 137 filled forms had been submitted back as responses. This is approximately a 62% response rate. This research survey response rate was adequate to make recommendations and conclusions of the study. According to Mugenda and Mugenda (2003) a 50 % response rate is considered adequate for data analysis. Based on this declaration, the received threshold is adequate to analyze.

Table 3 4.1; Response Rate Table

Rate	Frequency	Percentage
Forms filled and submitted	137	62%
Forms not submitted	83	38 %
Total	**122**	**100**

Source: Research Data (2021)

4.3 Demographics

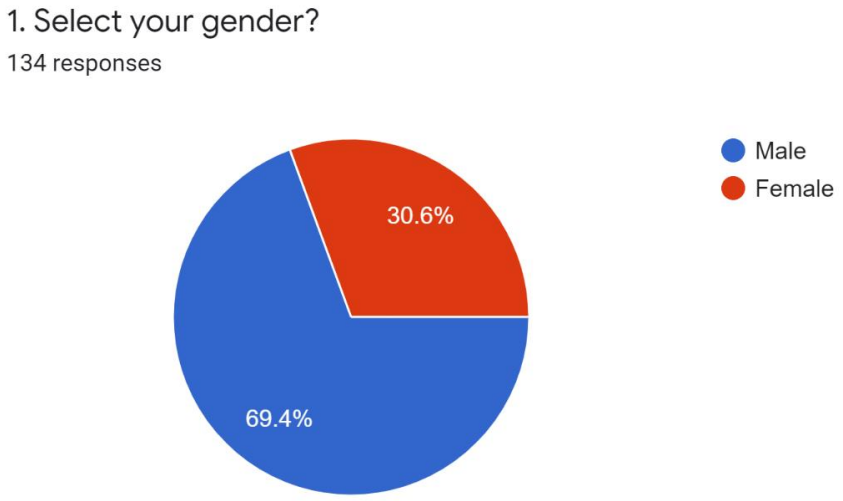
In this section the demographics are looked at in terms of the gender, age group, highest educational level, job position of the respondents and period of years the respondent had worked in their SACCO analyzed.

4.3.1 Gender of Respondents

On the received response out of the 69.4% (93) were submitted by male where as 30.6% (41) were attempted by female. It will be indeed correct to affirm that based on this finding's majority of employees in SACCOs offering Mobile money and related cybersecurity services are men.

It is therefore important that female counterparts should be supported to the cybersecurity roles in the SACCOs

Figure 5; The Gender of Respondents



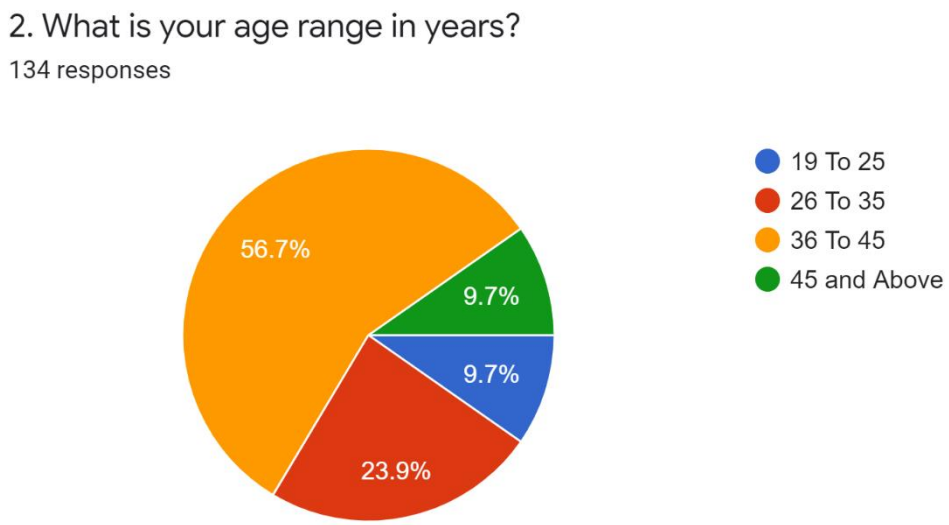
Source: Research Data (2021)

4.3.2 Age Group of the Respondents

The age group results show that there exists respondent from the age of 19 years to those who are 45 years and above. However, among the submitted responses the respondent of the ager 19 to 25 years were 9.7% (13) while the 26 to 35 years category were 23.9% (32), 36 to 45

years category were 56.7% (76) and those of 45 years and above category were 9.7% (13). This is an implication that the DT SACCOs mobile cybersecurity is dominated by young employees. They are robust, flexible and capable to adopt and run with rapid and dynamic technological innovations.

Figure 6 4.2; The Age Group of the Respondents

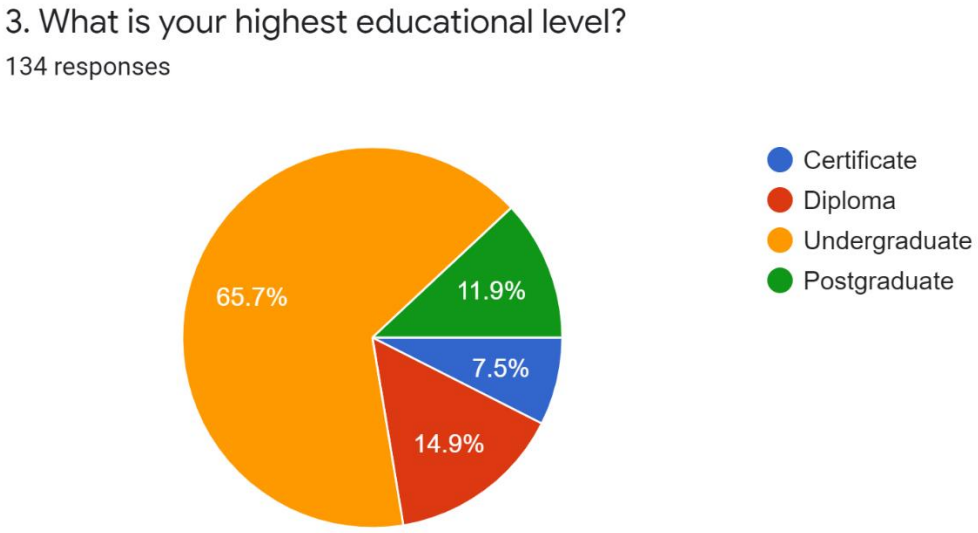


Source: Research Data (2021)

4.3.3 Highest Education Level of the Respondents

The highest respondent's education level was postgraduate degrees and this was represented by 11.9% (16). The undergraduate degree respondents dominate having a 65.7% (88) response. The diploma respondents were having a 14.9% (20) response and 7.5% (10) were having certificates. This demonstrated that most of the staff working in DT SACCO are educated and technically prepared to face the changing paradigm of technology and as well comply with the minimum job requirements in their respective SACCO and positions.

Figure 7; Highest Education Level

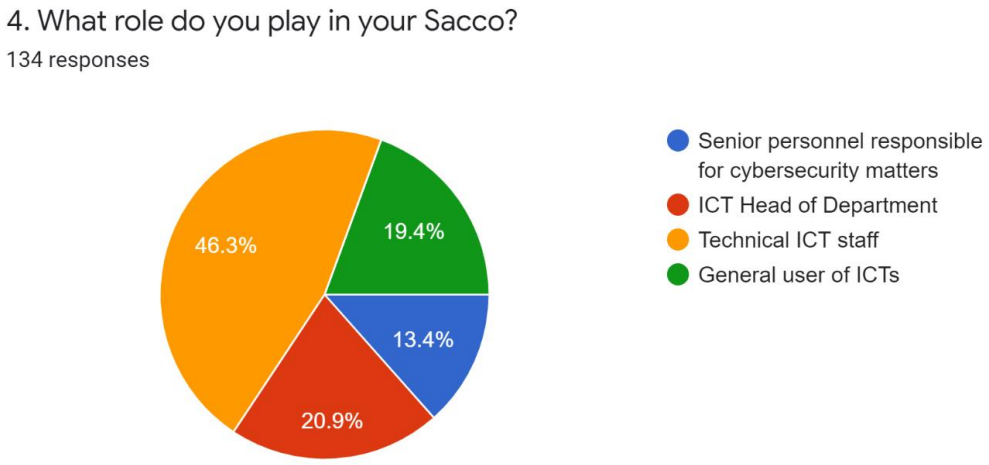


Source: Research Data (2021)

4.3.4 Job Positions

The research sample in this study remained a representative of all the levels of the SACCO structures which involved critical staff across SACCOs. 13.4% (18) of responses were Senior personnel responsible for cybersecurity matters, 20.9% (28) were ICT Head of Departments (HoDs), 46.3% (62) were Technical ICT staff and finally 19.4% (26) were General users of ICT.

Figure 8; Respondents Job Description

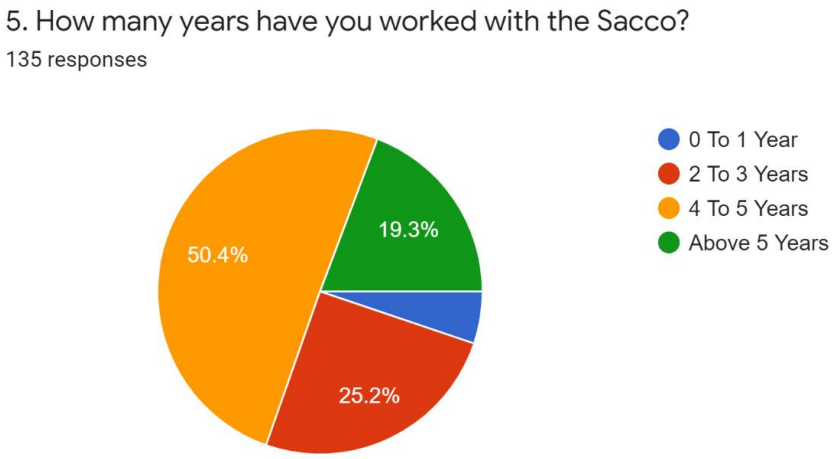


Source: Research Data (2021)

4.3.5 Respondents Working Experience

The study involved employees who had varying working experience in their workplaces. This was evidence in the diversity in their response. The experiences spanned from less than one year to over than five (5) years. Among the responses received 19.3% (26) respondents had work experience above five (5) years, 50.4% (68) respondents had work experience of between four (4) to five (5) years, 25.2% (34) respondents had work experience of between two (2) to Three (3) years and 5.2% (7) respondents had work experience of less than one (1) year.

Figure 9; Respondents Working Experience



Source: Research Data (2021)

4.4. Descriptive Analysis

The submitted response were analyzed by way of standard deviation (std Dev), mean and percentiles.

The respondents were given a five (5) point scale ranging from Strongly Disagree (SD), Disagree (D), Neutral (N), Agree (A) and Strong Agree (SA) from which they were required to pick responses that described cybersecurity situations in their respective SACCO.

4.4.1 Key Strategies of Mobile Money Cybersecurity Readiness

The research aimed at identifying mobile money cybersecurity strategies that the respondents supposed to have affected the cybersecurity readiness for mobile banking in their SACCOs in relevance to linking the findings of the empirical studies. The respondents were requested to respond to indicators of cybersecurity strategies delineated in the data forms that was data collection instrument if they believed these strategies had or had not contributed to cybersecurity readiness for mobile banking in their SACCO. From the figure 4.6, 99 of the respondents strongly agree and 28 agree that SACCO governance contribute to cybersecurity resilience. This makes majority of the respondents on this strategy believing that SACCO governance influence the mobile money cybersecurity readiness. 103 respondents agree while only 19 strongly agree that cybersecurity policies covering mobile banking strategies have affected the mobile money cybersecurity readiness. There were also a number of respondents who were neutral on this strategy but generally the majority respondents register positivity of cybersecurity policies covering mobile banking strategies contributing to the mobile money cybersecurity readiness.

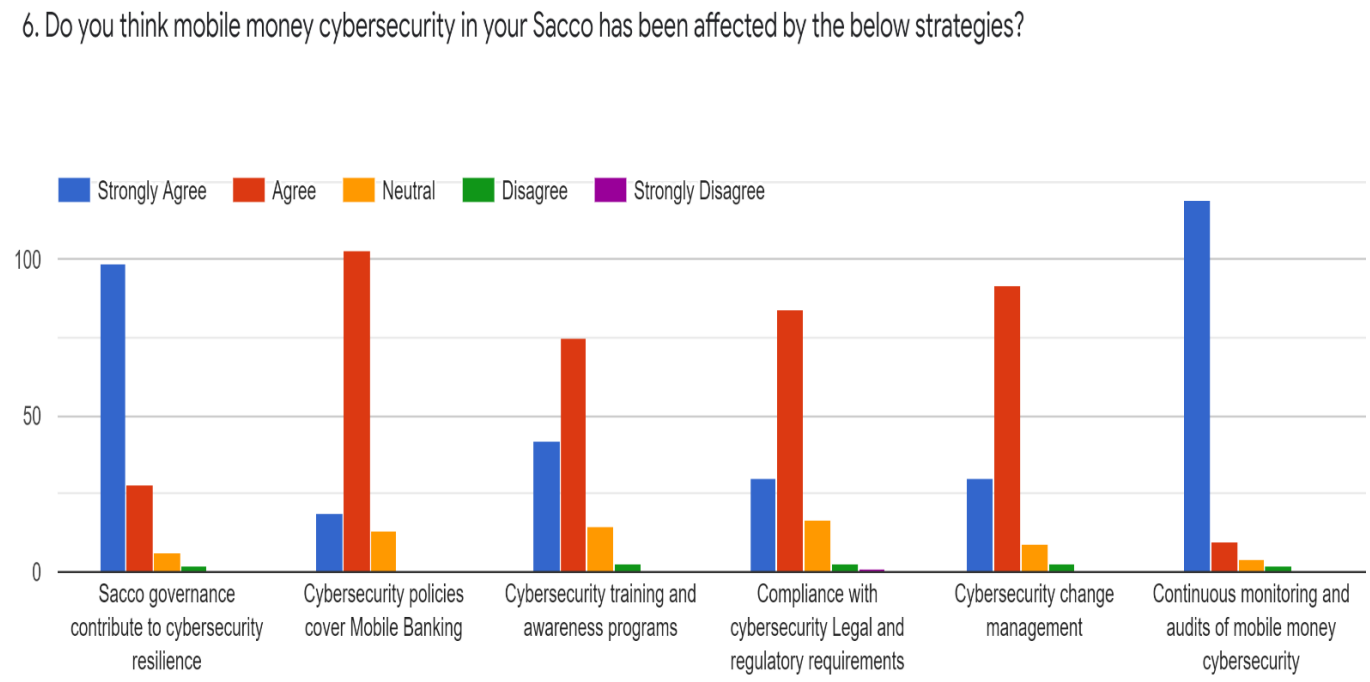
The respondents also acknowledged that cybersecurity training and awareness program affect mobile money cybersecurity readiness in their SACCOs where 75 respondents agreed and 42 of them strongly agreed making the majority of the responses in the positivity bracket. Compliance with cybersecurity legal and regulatory requirements strategy registered 84 respondents agreed while 30 strongly agreed that this strategy influence the mobile money cybersecurity readiness in their SACCOs. Despite having 17 respondents who were neutral the majority still believe in Compliance with cybersecurity legal and regulatory requirements strategy contributing to mobile money cybersecurity readiness.

Cybersecurity change management strategy had majority of the respondents believing this strategy influences mobile money cybersecurity readiness in their SACCO whereby 92 agreed

and 30 strongly agreed. The continuous monitoring and audits of mobile money cybersecurity strategy was the most highly rated strategy indicator registering 119 respondents strongly agreeing and 10 respondents agreeing. This is the majority positive response that continuous monitoring and audits of mobile money cybersecurity greatly influence mobile money cybersecurity readiness in their SACCO.

Based on the positive response from the respondents having the most strongly agreed strategy as continuous monitoring and audits of mobile money cybersecurity followed by others, this study recognized them as critical strategies affecting the mobile money cybersecurity readiness among the DTs SACCOs in Nairobi City County in Kenya.

Figure 10; Respondents on Strategies affecting Mobile Money Cybersecurity Readiness



Source: Research Data (2021)

4.4.2 Cybersecurity Practices in Respondents SACCO

The analysis in Table 4 demonstrate the way respondents view the general information about cybersecurity mobile banking in their SACCO.

Table 4; Respondents on cybersecurity practice;

Statements	SD	D	N	A	SA	TOTAL
Implementation of an effective mobile Banking cybersecurity readiness will reduce loss of resources in our SACCO	4.4%	0.7%	2.2%	31.9%	60.7%	100%
Inadequate governance support and involvement to Mobile Banking cybersecurity program prevent implementation of adequate mobile money Cybersecurity readiness in our SACCO.	1.5%	1.5%	5.2%	52.6%	39.3%	100%
Absence of cybersecurity policies adversely affects efforts towards achieving adequate Mobile Money Cybersecurity Readiness in our SACCO	2.2%	0.7%	3.7%	63.7%	29.6%	100%
Staff receive inadequate skills, training, and awareness programs on Mobile Money cybersecurity has result to inadequate Mobile Money cybersecurity in our SACCO	0.7%	2.2%	5.9%	68.9%	22.2%	100%
Lack of training and awareness to SACCO members on Secure mobile banking result in inadequate Mobile Money Cybersecurity Readiness	0.8%	1.5%	1.5%	72.2%	24.1%	100%
Premature automation technology levels adversely result in inadequate Mobile Money Cybersecurity Readiness in our SACCO	0.7%	2.2%	9.6%	74.8%	12.6%	100%
Nonexistence of audit and monitoring activities on cybersecurity of Mobile Banking has led to inadequate Mobile Money Cybersecurity Readiness in our SACCO	0.7%	1.5%	2.2%	40.7%	54.8%	100%

Source: Research Data (2021)

The responses indicate majority respondents agreed with the and strongly agree with the statements given. It was evident that there exists gaps between the best cybersecurity mobile banking and the current cybersecurity banking readiness that should achieved among the DTs SACCO. The results closely relate with the Africa Cybersecurity 2019/2020 Report surveyed

by Serianu which identified most of DTs SACCOs as not fully ready to deal with cybersecurity mobile banking.

Generally, most respondents believed that implementation of an effective mobile Banking cybersecurity readiness will reduce loss of resources in their SACCO with a score of strongly agree 60.7% and Agree of 31.9% followed by nonexistence of audit and monitoring activities on cybersecurity of Mobile Banking has led to inadequate Mobile Money Cybersecurity Readiness in their SACCO with a Strongly Agree of 54.8% and Agree of 40.7%.

4.4.3 Adequate mobile money Cybersecurity Readiness in SACCO

The instrument for this research study also focused on identifying the extent to which respondents agree or disagree on some statements determining the adequate mobile money cybersecurity readiness in the SACCO that the survey is taking place. The responses were recorded and tabulated in the Table 5 below.

Table 5; Descriptive Analysis for Adequate Mobile Money Cybersecurity Readiness

Statements	SD	D	N	A	SA	mean	Std Dev
There exist physical cybersecurity products like cybersecurity technologies (Hardware & Software) Firewall, access control system, Scanners and visual personnel security in our SACCO.	0.0%	1.5%	5.2%	84.3%	9.0%	4.1	0.45
There are presence of automated technologies for the SACCO such us Integration Mobile Money payments activities in our SACCO	0.0%	11.1%	19.3%	66.7%	3.0%	3.6	0.72
Staff possess the certifications and adequate mobile money Cybersecurity skills in our SACCO.	8.1%	25.2%	5.9%	58.5%	2.2%	3.2	1.10
SACCO members are aware of the risk associated with Mobile money services	19.3%	14.8%	10.4%	48.9%	6.7%	3.1	1.30
Cybersecurity availability is one of the desired cybersecurity values for our SACCO.	8.1%	17.0%	11.9%	57.0%	5.9%	3.4	1.09

I view Mobile Money Cybersecurity activities in our SACCO as NOT an overhead activity to my daily work routine	1.5%	12.6 %	16.3 %	60.0%	9.6%	3.6	0.8 8
If you had a cybersecurity threat, are you likely to be aware.	0.7%	3.0%	6.7%	67.4%	22.2 %	4.1	0.6 8
I clearly understand my roles & responsibilities relating to cybersecurity.	0.0%	1.5%	3.0%	47.8%	47.8 %	4.4	0.6 3
My employer understands my roles & responsibilities relating to cybersecurity.	0.7%	2.2%	5.2%	87.4%	4.4%	4.0	0.5 0
I understand the following policy topics as covered by the ICT/cybersecurity policy? I. Password II. E-mail III. Message IV. Virus, worms or malicious code V. Two Factor Authentication 2FA VI. Backup VII. IoT	0.0%	1.5%	3.7%	36.3%	58.5 %	4.4	0.6 3
Total Mean						3.79	

Source: Research Data (2021)

It was necessary to have the visible and tangible proof of the cybersecurity devices or equipment which acted as demonstration efforts towards achieving the mobile banking cybersecurity readiness. The study survey opined to establish this through the statement "There exist physical cybersecurity products like cybersecurity technologies (Hardware & Software) Firewall, access control system, Scanners and visual personnel security in our SACCO." Where most of the respondents agreed 84.3% and 9.0% strongly agreed creating the majority agreeableness of the presence of such products. Most of the gaps existed in the way respondent ability was The study survey also poised to understand the people factor like perception and on cybersecurity roles through the statements "I view Mobile Money Cybersecurity activities in our SACCO as NOT an overhead activity to my daily work routine" and majority of the respondents agreed 60% that cybersecurity is not an overhead role but indeed an all-round role for everyone in the SACCO. The response for the statement "My employer understands my roles & responsibilities relating to cybersecurity" was highly agreed with 87.4%. This is a clear demonstration of the expectation an employer could be having when it comes to mobile baking cybersecurity.

The response further revealed that there were presence of automated technologies for the SACCO such us Integration Mobile Money payments activities in our SACCO with a mean of 3.6 and that Staff possess the certifications and adequate mobile money Cybersecurity skills in SACCO with a mean of 3.2. The statement "I clearly understand my roles & responsibilities relating to cybersecurity" recorded the highest mean of 4.4 showing that most of the employees have broader understanding of their roles concerning the mobile money cybersecurity.

There was a largest standard deviation of 1.30 on "SACCO members are aware of the risk associated with Mobile money services" statement meaning there were varied response from SACCO to SACCO on the way the members of the SACCOs are made aware of the risks they face while transacting with mobile banking. The total mean for this section on adequate mobile money cybersecurity readiness in the SACCO is 3.79 which is high indicator that most of the respondents agreed with the statements.

4.4.4 SACCO Governance Support to Cybersecurity Resilience

The SACCO governance constitutes of the board of directors and top management (Not all of them) of the SACCO as it has been defined by the SASRA who is the SACCO regulatory agency of the government. The survey for this research study aimed at recognizing the extent to which respondents agree or disagree on some statements influencing the SACCO governance support to cybersecurity resilience. The response from the respondents indeed showed that SACCO governance support to cybersecurity resilience varied from SACCO to SACCO and from individuals in the same SACCO as well. The responses were recorded and tabulated in the Table 4.4 below.

From the table 6 below on SACCO Governance commit and approve adequate budget for cybersecurity activities only 0.7 % (1) strongly disagreed, 3% (4) disagreed, 5.2% (7) were neutral. The majority who were those who agreed being 82.2% (111) and 8.9% (12) strongly

agreed indicating a positivity rate on this statement. On the statements of "The SACCO Governance gives strong and consistent support towards adoption of adequate cybersecurity practices", "Top management regularly receive reporting on the status of cybersecurity status" and "The Board of management has the Sub-committee that frequently meet to deliberate on mobile money cybersecurity operations" have all shown a great positive agreeableness having the minimum of 77% as the lowest.

This statistics have as well agreed to the ISACA report 2019 which indicated that above 80% of SACCO governance are willing to adopt the mobile money cybersecurity preparedness and resilience.

Table 6; Descriptive Analysis for SACCO Governance Support to Cybersecurity Resilience

Statements	**SD**	**D**	**N**	**A**	**SA**	**mean**	**Std Dev**
SACCO Governance commit and approve adequate budget for cybersecurity activities	0.7%	3.0%	5.2%	82.2%	8.9%	4.0	0.57
The SACCO Governance gives strong and consistent support towards implementation of adequate mobile money cybersecurity practices	0.7%	5.2%	7.4%	79.3%	7.4%	3.9	0.64
Top management regularly receive reporting on the status of cybersecurity status	0.7%	3.0%	11.9%	77.8%	6.7%	3.9	0.60
The Board of management has the Sub-committee that frequently meet to deliberate on mobile money cybersecurity operations.	1.5%	4.4%	10.4%	77.0%	6.7%	3.8	0.68
Overall mean score						3.9	

Source: Research Data (2021)

4.4.5 Mobile money Cybersecurity Policies

The research study further pursued to evaluate the mobile money cybersecurity influence in mobile money cybersecurity readiness in DTs SACCOs. There was majority agreements with utmost statements on the mobile money cybersecurity related policies demonstrating an

implication that most of the DT SACCOs have developed and implemented these policies. The responses were recorded and tabulated in the Table 4.4 below.

Table 7; Descriptive Analysis of Mobile Money Cybersecurity Policies

Statements	SD	D	N	A	SA	mean	Std Dev
There are documented mobile money cybersecurity policies and guidelines that serves as a basis to inform shared cybersecurity and beliefs values	3.0%	4.5%	5.2%	81.3%	6.7%	3.84	0.734
Employees are aware, understand and accept ICT/Cybersecurity policy rules and guidelines	0.7%	3.0%	7.4%	83.0%	5.9%	3.90	0.558
Top management regularly receive reporting on the status of cybersecurity status	0.7%	3.0%	11.9%	77.8%	6.7%	3.87	0.596
Users of ICT systems including mobile services abide by ICT/cybersecurity policies.	3.0%	9.6%	10.4%	71.1%	5.9%	3.67	0.845
The ICT policy including cybersecurity for mobile money is regularly revised or updated	0.7%	3.7%	5.2%	82.2%	8.1%	3.93	0.588
Overall mean score						3.84	

Source: Research Data (2021)

From the table 7 above, apart from the majority agreeing with the minimum percentage of 71.1 from the statement "Users of ICT systems including mobile services abide by ICT/cybersecurity policies." the statement "Employees are aware, understand and accept ICT/Cybersecurity policy rules and guidelines" had the highest with agreeableness of 83.0% implying that the staff are well versed with current cybersecurity landscape as it relates to policies and are willing to live by the standards. The highest mean was recorded from the statements "The ICT policy including cybersecurity for mobile money is regularly revised or updated" of 3.93 showing that most of the respondents understand the dynamic changes that keep happening around mobile money technologies and hence important that the same are reflected in the policies of their DT SACCOs.

The figure 3.84 assumed the general mean on the mobile money cybersecurity policies demonstrating a high positivity response on it contribution to the mobie money cybersecurity readiness among the DT SACCOs.

4.4.6 Cybersecurity Skills, Training and Awareness programs

The cybersecurity skills, training and awareness is the backbone of the initiative to derive the whole scenario and environment both at individual and SACCO level. In this area the research evaluated the practices on the skills, training and awareness programs among the DT SACCO. The submitted responses were recorded and analyzed as shown in the Table 4.6 below.

Table 8; Descriptive Analysis of Cybersecurity Skills, Training and Awareness Program

Statements	**SD**	**D**	**N**	**A**	**SA**	**mean**	**Std Dev**
New employees are offered cybersecurity awareness programme in cybersecurity issues.	2.2%	3.0%	7.5%	82.8%	4.5%	3.84	0.647
Employees frequently receive training on mobile money cybersecurity that informs them on cybersecurity issues and consequences of cyber abuses	1.5%	20.1%	11.2%	64.2%	3.0%	3.47	0.899
The cybersecurity training programs are customized to individual awareness, technical difficulty or departmental risk profile	7.5%	25.6%	6.8%	57.9%	2.3%	3.22	1.089
Employees in our SACCO know and understand mobile money cybersecurity and other cybersecurity best practices and their application on real live situation.	2.2%	10.4%	10.4%	73.9%	3.0%	3.65	0.797
Overall mean score						3.55	

Source: Research Data (2021)

From the table 8, the responses submitted there was variance from SACCO to SACCO on the cybersecurity skills, training and awareness programs. The highest agreeableness was recorded on new employees being offered mobile money cybersecurity awareness programme of 82.8% and the lowest agreeableness of 57.9% from "The cybersecurity training programs are customized to individual awareness, technical difficulty or departmental risk profile"

statement. It was still the same statement registering the highest strongly disagree percentage of 7.5% .The total mean is 3.55 which has a positive implication that cybersecurity skills, training and awareness programs contribute greatly and the contrary have influence on the mobile money cybersecurity readiness among the DT SACCOs.

4.4.7 Legal and Regulatory compliance with Cybersecurity Requirements

The legal and regulatory framework is key to preventing and mitigating the related cybercrimes. In these section the study sought to understand the legal and regulatory compliance with cybersecurity requirements through the statements as enlisted and their response recorded in the Table 9 below. The responses recorded and tabulated showed a diverse perspective from SACCO to SACCO. There was also variance in the way respondents comply with the cybersecurity policies regulations and practices

Table 9; Descriptive Analysis of Legal and Regulatory Compliance with Cybersecurity Requirements

Statements	**SD**	**D**	**N**	**A**	**SA**	**mean**	**Std Dev**
There are not enough Government and industry cybersecurity regulations in Kenya	3.0%	26.7%	9.6%	58.5%	2.2%	3.30	0.987
Employee in our SACCO signs information security non- disclosure agreement during each new employee on boarding process.	3.0%	8.1%	5.9%	79.3%	3.7%	3.73	0.786
Cybersecurity regulations and practices are adhered to in our SACCO.	3.0%	16.3%	8.9%	67.4%	4.4%	3.54	0.920
Overall mean score						3.52	

Source: Research Data (2021)

From the table 9 on whether there are not enough Government and industry cybersecurity regulations in Kenya, majority with the percentage of 58.5 agreed pointing out that the government could have done much better in her regulatory agencies. The statement

"Employee in our SACCO signs information security non- disclosure agreement during each new employee on boarding process" the respondents had a high percentage of agree of 79.3 followed by Cybersecurity regulations and practices being adhered to in the SACCOs with 67.4%. The highest mean among the three statements was 3.73 and the general mean is 3.52 which is a positive implication that legal and regulatory compliance with cybersecurity requirement contributes to the mobile money cybersecurity readiness among the DT SACCO

4.4.8 Proactive Mobile Money Monitoring and Audit

The study finally focused to validate effectiveness of the proactive mobile money cybersecurity monitoring and audit on the cybersecurity mobile money readiness among the DT SACCOs. The statements in the table 10 were formulated and respondents gave their opinion. The responses submitted demonstrated a varied opinions from SACCO to SACCO on the degree of agreeableness and disagreeableness. The results were recorded as shown in the table 10 below.

Table 10; Descriptive Analysis of Proactive Mobile Money Monitoring and Audit

Statements	SD	D	N	A	SA	mean	Std Dev
Our SACCO routinely conduct mobile money cybersecurity audit and maintain data of cybersecurity vulnerability and intrusion attempts.	0.8%	9.8%	10.5%	72.2%	6.8%	3.75	0.755
There is mechanism to ensure effective monitoring of cybersecurity systems.	0.7%	11.2%	11.2%	72.4%	4.5%	3.69	0.760
There is mechanism in place to ensure effective monitoring of user violation of ICT/cybersecurity policies.	1.5%	13.4%	15.7%	64.9%	4.5%	3.57	0.835
Employees in our SACCO know and understand mobile money cybersecurity and other cybersecurity best practices and their application on real live situation.	0.7%	3.0%	3.7%	59.0%	33.6%	4.22	0.719
Overall mean score						3.81	

Source: Research Data (2021)

From the table 10 above on if the SACCOs routinely conducted mobile money cybersecurity audit and maintain data of cybersecurity vulnerability and intrusion attempts, those respondents who strongly agreed were 6.8%, agree were 72.2%. This is second highest agree after 72.4% which is recorded from the respondents on whether there was mechanism in place to ensure effective monitoring of cybersecurity systems. Thought the statement "Employees in our SACCO know and understand mobile money cybersecurity and other cybersecurity best practices and their application on real live situation" scored the lowest agreeableness of agree of 59.0% among the rest of the statements, it was noted that it had the most stable and highest mean of 4.22. This was followed by the 3.57 mean which came from the statement of whether there was a mechanism in place to ensure effective monitoring of user violation of cybersecurity policies.

The general mean for the proactive mobile money monitoring and audit statements was 3.81 which is positive and this statistics concludes the implication that proactive mobile money cybersecurity monitoring and audit contributes to the cybersecurity mobile money readiness among the DT SACCOs where the survey was done.

4.5 Inferential Statistics

The study has included this inferential statistics to support the survey draw conclusion based on the data that has actually been measured. In the inferential statistics the Pearson correlation analysis methods and multiple regression analysis methods were included in this study.

4.5.1 Normality Test

The Test of Normality was carried out to determine the assumption of parametric testing on the Linkert scale data. Two tests were carried out one of them being the Kolmogov-Smirnov and Shapiro-Wilk that are found in the SPSS and are mostly recommended for the data whose set

is less than 100. in the normality test the null hypothesis tends to be normally distributed. The data was not normally distributed since the statistical significance for Shapiro-Wilk is more than 0.5. This case subjected the collected data to ordinal regression analysis and Pearson correlations to be carried out on the non-parametric data

Table 11: Test of Normality Table

Tests of Normality[a,b]

	Sacco Governance Support and Contribution to Cybersecurity Programs	Kolmogorov-Smirnov[c]			Shapiro-Wilk
		Statistic	df	Sig.	Statistic
Adequate Mobile Money Cybersecurity Readiness	2.33	.260	2	.	
	2.67	.260	2	.	
	3.00	.265	3	.	.953
	3.33	.207	6	.200*	.952
	3.67	.239	12	.056	.860
	4.00	.216	92	<.001	.913
	4.33	.191	11	.200*	.922
	4.67	.260	2	.	
	5.00	.385	3	.	.750

Source: Data 2021

4.5.2 Correlation Analysis

The study variables' relationship was established by correlation analysis. The Pearson correlation coefficient was identified and used in this study. This was contributed by the nature of the data which had interval such as the mean of the Likert scale from the questionnaire (McLeod, 2019). The correlation amongst a number of cybersecurity variables and adequate mobile money cybersecurity readiness was calculated and obtained in the table 11.

Table 11; Pearson Analysis of Proactive Mobile Money Monitoring and Audit Correlations

Pearson Analysis of Proactive Mobile Money Monitoring and Audit ***Correlations***							
		(X_1)	**(X_2)**	**(X_3)**	**(X_4)**	**(X_5)**	Y
SACCO Governance Support and Contribution to Cybersecurity Programs **(X_1)**	Pearson Correlation	--					
	N	135					
Mobile Money Cybersecurity Policies**(X_2)**	Pearson Correlation	.507**	--				
	Sig. (2-tailed)	<.001					
	N	135	135				
Cybersecurity Skills, Training and Awareness Programs**(X_3)**	Pearson Correlation	.415**	.345**	--			
	Sig. (2-tailed)	<.001	<.001				
	N	134	134	134			
Legal & Regulatory Compliance with Cybersecurity Requirements**(X_4)**	Pearson Correlation	.271**	.444**	.510**	--		
	Sig. (2-tailed)	.002	<.001	<.001			
	N	135	135	134	135		
Proactive Mobile Money Monitoring & Audit**(X_5)**	Pearson Correlation	.472**	.397**	.538**	.604**	--	
	Sig. (2-tailed)	<.001	<.001	<.001	<.001		
	N	134	134	134	134	134	
Adequate Mobile Money Cybersecurity Readiness-Y	Pearson Correlation	.368**	.430**	.514**	.472**	.589**	--
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	
	N	135	135	134	135	134	135
**. Correlation is significant at the 0.01 level (2-tailed).							

Source: Research Data (2021)

Results and findings demonstrated that the adequate mobile money cybersecurity readiness correlated positively with the independent variables. This positive correlation implies that the increase in the independent variables will reflect the corresponding increase in the adequate mobile money cybersecurity readiness and the decrease in the independent variables reflect the corresponding decrease in the adequate mobile money cybersecurity readiness.

From the above Table 4.8; p-values amongst variables of the study and the correlation coefficients have been shown through Pearson correlation matrix. The statistics in this inferential analysis is case based where all cases assessed there above are cases with no missing

values for any variable used. The results demonstrate that the SACCO Governance Support and Contribution to Cybersecurity Programs and Adequate Mobile Money Cybersecurity Readiness scored a correlation of r= 0.368 ($p < 0.001$) implying that the SACCO Governance Support and Contribution to Cybersecurity Programs is greatly significant in contributing to the adequate Mobile Money Cybersecurity Readiness. It is therefore critical to invest and plan a good governance structures among SACCOs since they will increasingly reflect the growth in the adequate Mobile Money Cybersecurity Readiness.

The analyzed results from the table also show that Mobile Money Cybersecurity Policies and adequate Mobile Money Cybersecurity Readiness had a Pearson correlation coefficient of r= 0.430 ($p < 0.001$). This suggests that Mobile Money Cybersecurity Policies positively correlates with adequate Mobile Money Cybersecurity Readiness. A positive change will positively reflect the corresponding increase in the adequate Mobile Money Cybersecurity Readiness. The reduction or the negative change will also reflect the corresponding decrease in the adequate Mobile Money Cybersecurity Readiness.

The Pearson correlation between Cybersecurity Skills, Training and Awareness Programs and adequate Mobile Money Cybersecurity Readiness with the correlating coefficient of $r = 0.514$ ($p < 0.001$) demonstrate a positive and significant association between Cybersecurity Skills, Training and Awareness Programs and adequate Mobile Money Cybersecurity Readiness. The increase in Cybersecurity Skills, Training and Awareness Programs will reflect the corresponding increase in the adequate Mobile Money Cybersecurity Readiness.

Legal & Regulatory Compliance with Cybersecurity Requirements variable with the Pearson coefficient of $r = 0.472$ ($p < 0.001$) absolutely and expressively correlates with the adequate Mobile Money Cybersecurity Readiness. This implies that the increase in the Legal &

Regulatory Compliance with Cybersecurity Requirements will reflect a corresponding increase in the adequate Mobile Money Cybersecurity Readiness and the reverse is also true.

Finally, there exists an expressively important correlation between Proactive Mobile Money Monitoring & Audit and adequate Mobile Money Cybersecurity Readiness represented by a correlation coefficient $r = 0.589$ ($p < 0.001$). The increase in the Proactive Mobile Money Monitoring & Audit will lead to the corresponding increase in the adequate Mobile Money Cybersecurity Readiness.

From the above fact finding all the factors have been based on the p-values that are less than 0.001. This is the most strong significant coefficient output in the correlation. The summary for correlation is shown in the Table 12 below;

Table 12; Correlation output Interpretation summary

Independent Variable	**The dependent Variable**	**Correlation Value(r)**	**Direction**	**Significance**
SACCO Governance Support and Contribution to Cybersecurity Programs	Adequate Mobile Money Cybersecurity Readiness	.368	Positive	<0.001 Very strong significance
Mobile Money Cybersecurity Policies		.430	Positive	<0.001 Very strong significance
Cybersecurity Skills, Training and Awareness Programs		.514	Positive	<0.001 Very strong significance
Legal & Regulatory Compliance with Cybersecurity Requirements		.472	Positive	<0.001 Very strong significance
Proactive Mobile Money Monitoring & Audit		.589	Positive	<0.001 Very strong significance

Source: Research Data (2021)

4.5.3 Regression Analysis

The research being quantitative the regression analysis was selected as the reliable method for identifying how the independent variable impact the dependent variable and also determine which factor matter most and which ones can be ignored in the whole model. The regression analysis was conducted to yield valuable, actionable insights on the Adequate Mobile Money Cybersecurity Readiness. There is need to know the factors to control and determine the confidence to have in the hypothesis.

The study conducted multiple regression analysis to establish how the SACCO Governance Support and Contribution to Cybersecurity Programs, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity Requirements and Proactive Mobile Money Monitoring & Audit factors jointly influence Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs in Nairobi City County in Kenya. The model summary of the multiple linear regression on Adequate Mobile Money Cybersecurity Readiness is shown in the Table 13.

From the model summary table below it is demonstrated that all the factors in the independent variable constituted 43.3% (R-Square = .433) of deviations in Adequate Mobile Money Cybersecurity Readiness (dependent variable). 56.7% of the variation in Adequate Mobile Money Cybersecurity Readiness was not explained and was dealt by factors that were not considered in this study research.

Table 13; Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.658[a]	.433	.411	.36025
a. Predictors: (Constant), Proactive Mobile Money Monitoring & Audit, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, SACCO Governance Support and Contribution to Cybersecurity Programs, Legal & Regulatory Compliance with Cybersecurity Requirements				

Source: Research Data (2021)

The ANOVA results alternatively show that F-statistics = 19.698 and also a corresponding p-value <.001. The analysis on the findings clearly demonstrate the predictive activities on adequate Mobile Money Cybersecurity Readiness among the DT SACCOs was statistically significant. The model with best fitness that is suitable to envisage impact of the SACCO Governance Support and Contribution to Cybersecurity Programs, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity Requirements and Proactive Mobile Money Monitoring & Audit on the Adequate Mobile Money Cybersecurity Readiness among the DT SACCO in Nairobi City County.

Table 14; ANOVA Results

ANOVA[a] Results						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.782	5	2.556	19.698	<.001[b]
	Residual	16.742	129	.130		
	Total	29.524	134			
a. Dependent Variable: Adequate Mobile Money Cybersecurity Readiness						
b. Predictors: (Constant), Proactive Mobile Money Monitoring & Audit, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, SACCO Governance Support and Contribution to Cybersecurity Programs, Legal & Regulatory Compliance with Cybersecurity Requirements						

Source: Research Data (2021)

The results from the Table 14 illustrate the regression coefficients used in this study research. The regression model was adopted to envisage the Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs. The regression quantities are denoted by the β standards.

Table 15; Regression Coefficients

Regression Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		β	Std. Error	Beta		
1	(Constant)	1.307	.293		4.455	<.001
	SACCO Governance Support and Contributions	.005	.082	.005	.057	.955
	Mobile Money Cybersecurity Policies	.162	.073	.183	2.210	.029
	Cybersecurity Skills, Training and Awareness Programs	.174	.064	.226	2.700	.008
	Legal & Regulatory Compliance with Cybersecurity Requirements	.047	.071	.061	.667	.506
	Proactive Mobile Money Monitoring & Audit	.277	.073	.354	3.814	<.001
a. Dependent Variable: Adequate Mobile Money Cybersecurity Readiness						

Source: Research Data (2021)

Optimal Model

$$Y = \mathbf{1.307} + \mathbf{0.005}\ X_1 + \mathbf{0.162}\ X_2 + \mathbf{0.174}\ X_3 + \mathbf{0.047}\ X_4 + \mathbf{0.277}\ X_5 + \boldsymbol{\varepsilon}$$

$Y =$ Adequate Mobile Money Cybersecurity Readiness

X_1 = SACCO Governance Support and Contributions

X_2 = Mobile Money Cybersecurity Policies

X_3 = Cybersecurity Skills, Training and Awareness Programs

X_4 = Legal & Regulatory Compliance with Cybersecurity Requirements

X_5 = Proactive Mobile Money Monitoring & Audit

$\boldsymbol{\varepsilon}$ = Error term

4.6 Discussion of the Findings

4.6.1 Cyber Security Readiness for Mobile Banking

The research findings in the sections 4.4.1 to 4.4.8 acknowledged SACCO Governance Support and Contribution to Cybersecurity Programs, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity Requirements and Proactive Mobile Money Monitoring & Audit as key strategies that impacts cyber security readiness for mobile banking among the DT SACCOs surveyed.

Based on the regression analysis output as demonstrated in Table 12 illustrates that SACCO Governance Support and Contribution to Cybersecurity Programs represent a regression coefficient of $\beta = 0.005$ and $p = 0.955$ implying that SACCO Governance Support and Contribution positively and not significantly predicted adequate Mobile Money Cybersecurity Readiness. For every one increase on SACCO Governance Support and Contribution there could be an increase of 0.005 units in adequate Mobile Money Cybersecurity Readiness. This value is pretty infinite and hence unreliable to fully rely on it. The result also show that Mobile Money Cybersecurity Policies presented a regression coefficient of $\beta = 0.162$ and $p = 0.029$ implying that Mobile Money Cybersecurity Policies certainly and meaningfully predicted the adequate Mobile Money Cybersecurity Readiness. For every one unknit increase in Mobile Money Cybersecurity Policies there is a predicted increase of 0.162 units in the log odds of falling at a higher level on the adequate Mobile Money Cybersecurity Readiness.

Cybersecurity Skills, Training and Awareness Programs demonstrated a regression coefficient of $\beta = 0.174$ and $p = 0.008$ implies that an odd ratio 0.008 is > 1 suggests an increasing probability in a higher level on the adequate Mobile Money Cybersecurity Readiness as values on Cybersecurity Skills, Training and Awareness Programs increase. Legal & Regulatory Compliance with Cybersecurity Requirements presented a regression coefficient of $\beta = 0$ .047

and p = 0.506 implying that Legal & Regulatory Compliance with Cybersecurity Requirements positively and not significantly predicted the adequate Mobile Money Cybersecurity Readiness. One unit increase in Legal & Regulatory Compliance with Cybersecurity Requirements would lead to an increase of 0.047 in the adequate Mobile Money Cybersecurity Readiness.

Proactive Mobile Money Monitoring & Audit strategy as initially considered critical at the center of the research study presented the regression coefficient of $\beta = 0.277$ and $p < .001$ implying that whereas <1 in the probability suggests a decreasing probability with increasing values of Proactive Mobile Money Monitoring & Audit as it reflects on the adequate Mobile Money Cybersecurity Readiness.

As noted from the above discussion, all the hypotheses tested were in line with earlier study work.

Table 16 below summarizes the study hypotheses and the testing results.

Table 16; Summary of Hypothesis Testing

S/No	Relationship	Hypothesis	Result
1	SACCO Governance Support and Contribution	H1	Supported
2	Mobile Money Cybersecurity Policies	H2	Supported
3	Cybersecurity Skills, Training and Awareness Programs	H3	Supported
4	Legal & Regulatory Compliance with Cybersecurity Requirements	H4	Supported
5	Proactive Mobile Money Monitoring & Audit	H5	Supported

Source: Research Data (2021)

4.6.2 Blue Print for Mobile Banking Cybersecurity Readiness among DT SACCOs in Nairobi City County in Kenya

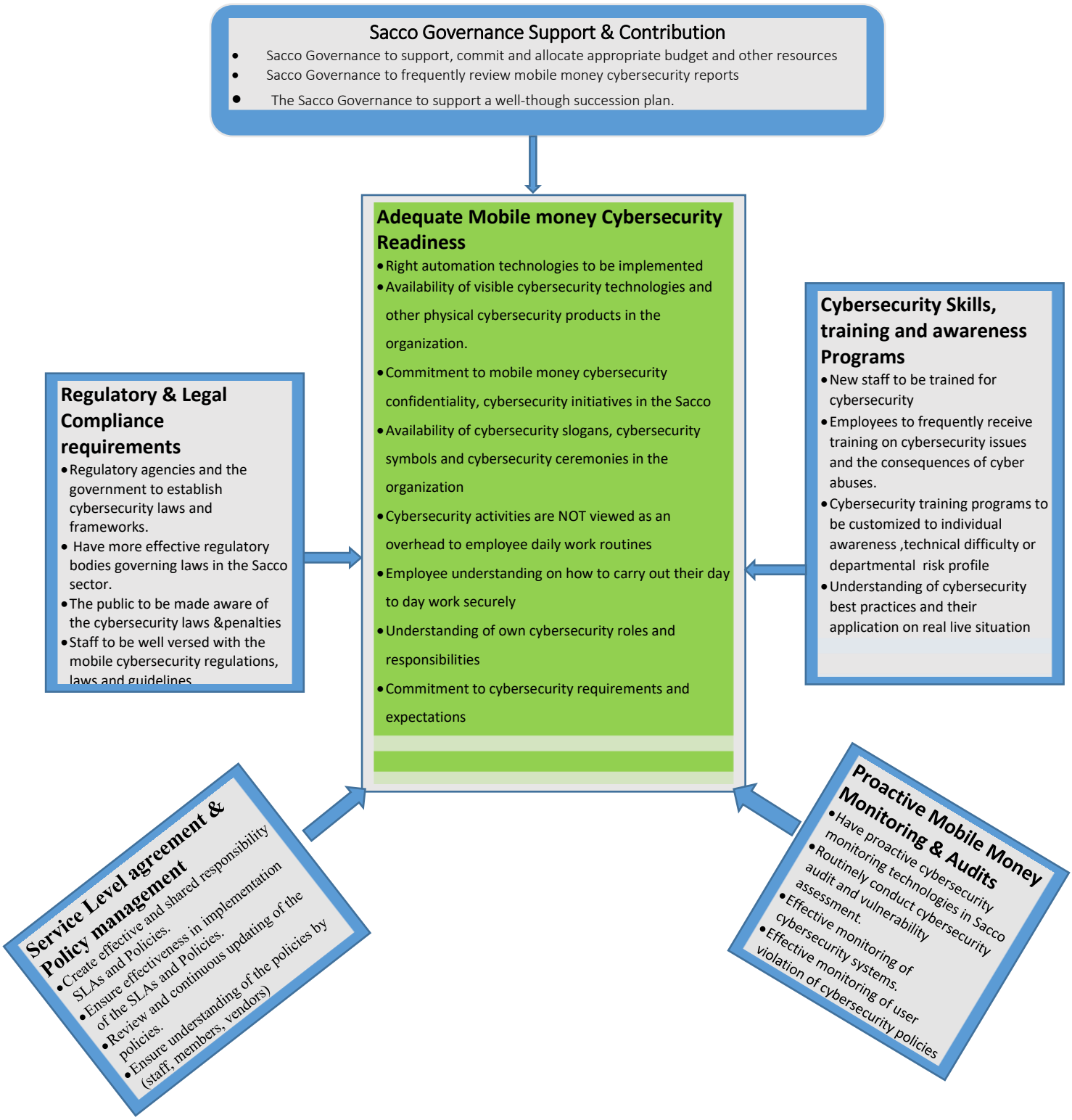
Based on the previous findings from the data and the discussion both on regression analysis and correlation, SACCO Mobile Money Service Level Agreement and Policy management, Cybersecurity Skills, Training and Awareness Programs, Proactive Mobile Money Monitoring & Audit strategies positively and significantly predicted adequate Mobile Money Cybersecurity Readiness. SACCO Governance Support and Contribution and Legal & Regulatory Compliance with Cybersecurity Requirements that positively but not significantly predicted the adequate Mobile Money Cybersecurity Readiness. This is because the data was not statistically significant demonstrated by the p-values were greater than 0.05. Statistically all the set hypotheses that had been set earlier by the study were accepted

The model has been considered adequate since the regression analysis results, in collaboration with descriptive analysis findings have been used to develop the adequate Blue Print for Mobile Banking Cybersecurity Readiness among the DT SACCOs. This was also the main objective for the study research. The Blue Print for Mobile Banking Cybersecurity Readiness proposed and developed has been subsequently based on practically existing measures, questions responded to in the study questionnaire and subsequent analysis.

Though the Blue Print for Mobile Banking Cybersecurity Readiness has been developed from the survey on the DT SACCOs in Nairobi City County of Kenya, it can be applied to the rest of DT SACCOs in Kenya and the rest of the world for adequate Mobile Money Cybersecurity Readiness. The Blue Print for Mobile Banking Cybersecurity Readiness can as well be used by the practitioners of cybersecurity and other professionals looking into winning strategies from the key financial industry players like those from Banks.

The Blue Print for Mobile Banking Cybersecurity Readiness among DT SACCOs in Nairobi City County in Kenya as shown in the figure 11 illustrates the main constructs as identified with their specific initiative that are used as metrics to evaluate support. The initiatives are the Key Performance Indicators- KPI of that construct for instance on the SACCO Governance Support and Constructions will be determined by how SACCO Governance support, commit and allocate appropriate budget and other resources, frequently review mobile money cybersecurity reports and support a well-though succession plan. The same is demonstrated in the rest constructs.

Figure 11; Blue Print for Mobile Banking Cybersecurity Readiness among DT SACCOs in Nairobi City County in Kenya



Adequate Mobile Money Cybersecurity Readiness

The Blue Print for Mobile Banking Cybersecurity Readiness diagram above, the proposed Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs that is at the center

in green will consist of the properties inside the construct. The properties are not sequential and they may be gauged in the order the SACCOs implements. The Adequate Mobile Money Cybersecurity Readiness will be characterized by; Right automation technologies to be implemented; Availability of visible cybersecurity technologies and other physical cybersecurity products in the organization; Commitment to mobile money cybersecurity confidentiality, cybersecurity initiatives in the Sacco; Availability of cybersecurity slogans, cybersecurity symbols and cybersecurity ceremonies in the organization; Cybersecurity activities are NOT viewed as an overhead to employee daily work routines; Employee understanding on how to carry out their day to day work securely; Understanding of own cybersecurity roles and responsibilities and Commitment to cybersecurity requirements and expectations.

The relationship of the Adequate Mobile Money Cybersecurity Readiness is affected by the other underpinning mobile money cybersecurity strategies. The arrows in the diagram all point to Adequate Mobile Money Cybersecurity Readiness since it is the depended variable to be achieved and the effect in the other variables will cause the corresponding effort.

Sacco Governance Support & Contribution

The SACCO Governance Support and Contribution has to show positive efforts to the Adequate Mobile Money Cybersecurity readiness by ensuring the following; Sacco Governance to support, commit and allocate appropriate budget and other resources; Sacco Governance to frequently review mobile money cybersecurity reports; The Sacco Governance to support a well-though succession plan. The efforts should be drawn and exercise high sense of the above practices to achieve the intended Adequate Mobile Money Cybersecurity. The properties don't portray any form of order and therefore they may be approached by the DT SACCO in any perspective that allows it to.

Service Level agreement & Policy management

The Service Level Agreements are very key in achieving the Adequate Mobile Money Cybersecurity Readiness. This as the strategy in this Blue Print for Mobile Banking Cybersecurity Readiness diagram. The area requires that any Service Level Agreement to; Create effective and shared responsibility Service Level Agreement -SLAs and Policies and ensure effectiveness in implementation of the Service Level Agreement SLAs and Policies.

The DT SACCOs Policy management deals with the set policy guidelines developed and updated and implemented in the SACCO. The Blue Print for Mobile Banking Cybersecurity

Readiness requires that; Review and continuous updating of the policies; Ensure understanding of the policies by (staff, members, vendors)- will contribute to the Adequate Mobile Money Cybersecurity Readiness among the DT SACCO.

Cybersecurity Skills, training and awareness Programs

Cybersecurity Skills, training and awareness Programs being a strategy to the Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs is concerned to promote that same by activities as; New staff to be trained for cybersecurity; Employees to frequently receive training on cybersecurity issues and the consequences of cyber abuses; Cybersecurity training programs to be customized to individual awareness, technical difficulty or departmental risk profile and understanding of cybersecurity best practices and their application on real live situation. The above activities are the continuous and apart from the new staff being trained for cybersecurity first the rest do not have the order by which they are to be undertake by the DT SACCO.

Regulatory & Legal Compliance requirements

Though the Regulatory & Legal Compliance requirements has been considered to have less significance it is still an underpinning strategy in achieving the Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs. For the Blue Print for Mobile Banking Cybersecurity Readiness the below activities will positively contribute; Regulatory agencies and the government to establish cybersecurity laws and frameworks; Have more effective regulatory bodies governing laws in the Sacco sector; The public to be made aware of the cybersecurity laws and penalties and Staff to be well versed with the mobile cybersecurity regulations, laws and guidelines

Proactive Mobile Money Monitoring & Audit

Proactive Mobile Money Monitoring & Audit in the Blue Print for Mobile Banking Cybersecurity Readiness diagram above has been focused from the base as it reserves important activities that ensures the positive contribution to the Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs. The activities are; Have proactive cybersecurity monitoring technologies in Sacco; routinely conduct cybersecurity audit and vulnerability assessment; Effective monitoring of cybersecurity systems and effective monitoring of user violation of cybersecurity policies. The strategy has been considered the baseline due to integration of both people process and technology.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter has covered subtopics that range from Summary of the findings of the research presented, Conclusions and Recommendations contained in this study research. The scope of the below conclusions is limited to the frameworks of mobile banking cybersecurity and characteristics of the DT SACCO industry hence, if it is applied to a different situation the conclusion could lead to incorrect outcomes. The presented summary of the significant results here are also pecked on the specific objectives and their respective questionnaires illustrating how the research study responded to the questionnaire.

5.2 Summary of Findings

The initial objective purposed to identify and review mobile money frameworks in DT SACCOs in the Nairobi City County in Kenya. The research questions in part A 6 "Do you think Mobile Money Cybersecurity in your SACCO has been affected by the below Strategies? Question (1-7)" and Part B; Identify and review the Mobile Money frameworks in place (questions 1- 8) of the questionnaire met identify and review mobile money frameworks among the DT SACCOs in Nairobi City County in Kenya met this objective. There was also need to identify the extent to which these frameworks influence the mobile money cybersecurity readiness in the DTs SACCO and this was achieved through the inferential statistics. The submitted responses from the questionnaire demonstrated the most critical frameworks that influence the mobile money readiness among the DT SACCO in Nairobi City County in Kenya. Based on the data from the respondents, the outputs from the regression analysis demonstrated the results.

Throughout the literature review, it was also reviewed and established that mobile money being a fast growing technology had not given a keen focus on the cybersecurity frameworks that

could safeguard its preparedness among the DT SACCO industry. SACCO Governance Support and Contribution, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity Requirements and Proactive Mobile Money Monitoring & Audit were recognized as being the critical strategies influencing Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs in Nairobi City County in Kenya. All the above strategies demonstrated positive relationship towards the Adequate Mobile Money Cybersecurity Readiness among the DT SACCOs. All the frameworks were positively and significantly predicted adequate Mobile Money Cybersecurity Readiness except the SACCO Governance Support and Contribution and Legal & Regulatory Compliance with Cybersecurity Requirements that positively but not significantly predicted the adequate Mobile Money Cybersecurity Readiness. The comprehensive results were presented in chapter four of this study.

Secondly, the research study objective was also to identify the most Adequate Mobile Money Cybersecurity Blue Print that will improve Mobile Money Cybersecurity Readiness for DT SACCO in Nairobi City County and the rest of the DT SACCOs in Kenya. The research questions in part C; "Adequate Mobile Money Cybersecurity Readiness questions from 1- 10 for DT SACCOs in Nairobi City County in Kenya. The objective was covered in the chapter four section where the validated data went through multiple regression and analysis that also extended to the descriptive analysis. The analysis on the findings both at descriptive and regression on the data harvested using the data collection instrument discovered varying Mobile Money Cybersecurity Readiness among the DT SACCOs studied. The varied responses from the data and the multiple regression analysis informed the development of the most adequate Blue Print. This Blue Print was developed and offered in figure 4. In chapter four of this research study.

The Proactive Mobile Money Monitoring & Audit was the most applauded strategy in enhancing and impacting Mobile Money Cybersecurity Readiness among the DT SACCO in the Nairobi City Count in Kenya. Based on the descriptive analysis it performed a well among the rest having the highest strongly agree response as shown in section 4.4.1 of the chapter four of this research study. This has implied a finding that most of the DT SACCO emphasize on Proactive Mobile Money Monitoring & Audit as the most effective strategy in for achieving Mobile Money Cybersecurity Readiness in their SACCOs.

The evaluation of the key factors that demonstrate Mobile Money Cybersecurity Readiness objective was also critical in this research study. It was substantially addressed under the literature review section in chapter three of this study research. Among the evaluated ones governance, technologies, and skills were the underpinning perspectives at all levels of the DT SACCOs in Nairobi City County of Kenya. The objective was also emphasized in the descriptive analysis where the validated data from the respondents gave the research varied perspectives ranging from one SACCO to the other.

5.3 Conclusion and Recommendations

The aim of the research study was to develop a cybersecurity blue print on Mobile Money Cybersecurity Readiness among SACCOs in Nairobi County by identifying a more suitable roadmap to implement the framework in the SACCO. A qualitative process of methodology was adopted by means of corresponding methods. The research study has discovered frameworks and strategies DT SACCOs can adopt to achieve adequate Mobile Money Cybersecurity Readiness. It also discovered a varied disagreeableness and agreeableness of the strategies from DT SACCO to another and how those strategies impact the achievements of the Mobile Money Cybersecurity Readiness.

Previous research studies on Cybersecurity identified frameworks and strategies ranging from SACCO Governance Support and Contribution, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs, Legal & Regulatory Compliance with Cybersecurity as the most critical strategies to be focused on by any financial institutions like DT SACCOs looking to achieve adequate Mobile Money Cybersecurity Readiness. It is also conclusive to mention that most researches focusing on cybersecurity did not keenly focus on the Mobile Money but was on cybersecurity generality. This makes the Mobile Money Cybersecurity Readiness and its adequacy the work in progress based on the rapid mobile money technologies around mobile money (GSMA, 2020).

However, this study was considered relatively small scale tentative research study, the assurance in generalizability strategy findings is greater based on the consistence in the findings, acquired by way of multiple processes and methods and most of the critical one the consensus among the participants. Though there are other frameworks and strategies that may as well be employed to achieve the Mobile Money Cybersecurity Readiness among the DT SACCO, the five studied herein primarily, are not to be considered discrete since they overlap and compliment others which might not have been mentioned here. This has allowed other topics and subtopics for future research and intervention.

The Proactive Mobile Money Monitoring & Audit strategy has been proven critical in this research study hence recommendable that beside other strategies like SACCO Governance Support and Contribution, Mobile Money Cybersecurity Policies, Cybersecurity Skills, Training and Awareness Programs and Legal & Regulatory Compliance, ought to be intensely looked into and be upheld by the DT SACCOs. It is also worthy to mention that since the DT SACCOs operations are nearly of the same model, the strategies are generic hence the findings in this study might easily apply across the DT SACCOs even those

outside the area of study. The recommendations given herein may as well extend with reservation in the results in case of variance in underpinning conditions.

5.4 Suggestion for further Research

The research study work concentrated on the Mobile Money Cybersecurity Readiness among DT SACCOs in Nairobi City County in Kenya. The study demonstrated 43.3% of the strategies accounted for adequate Mobile Money Cybersecurity Readiness. Further research studies ought to emphasis on a broader scope to demonstrate the outstanding 56.7% disparity among the adequate Mobile Money Cybersecurity Readiness in DT SACCOs. It is also considerable for further research to cover a more wide geographic area.

6.0 REFEREES

14:00-17:00. (n.d.). *ISO/IEC 27032:2012*. ISO. Retrieved December 3, 2020, from https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/43/44375.html

Adaba, G. B., & Ayoung, D. A. (2017). The development of a mobile money service: An exploratory actor-network study. *Information Technology for Development*, *23*(4), 668–686. https://doi.org/10.1080/02681102.2017.1357525

Calder, A., & Watkins, S. (2012). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. Kogan Page Publishers.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

Cyber security challenges to mobile banking in SACCOs in Kenya.pdf. Nambiro, 2017 Mobile phones for financial inclusion: What explains the diffusion of mobile money innovations?

Cybersecurity for Mobile Financial Services: A Growing Problem. (n.d.). Retrieved December 2, 2020, from https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem

cybersecurity on mobile money—Google Search. (n.d.). Retrieved December 4, 2020, from https://www.google.com/search?sxsrf=ALeKk02x1Fw27eyXynxjos9Zz1FTcdUDRA%3A1607029508454&source=hp&ei=BFPJX4S0GcKzgweagJrQDA&q=cybersecurity+on+mobile+money&oq=cybersecurity+on+mobile+money&gs_lcp=CgZwc3ktYWIQA1AAWABgAmgAcAB4AIABAIgBAJIBAJgBAKoBB2d3cy13aXo&sclient=psy-ab&ved=0ahUKEwiExvi327LtAhXC2eAKHRqABsoQ4dUDCAw&uact=5

Cybersecurity: A governance framework for mobile money providers. (2019, September 11). *Mobile for Development*.

https://www.gsma.com/mobilefordevelopment/blog/cybersecurity-a-governance-framework-for-mobile-money-providers/

Cybersecurity-A-governance-framework-for-mobile-money-providers_WEB.pdf. (n.d.). Retrieved December 3, 2020, from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/Cybersecurity-A-governance-framework-for-mobile-money-providers_WEB.pdf

Definition of Cybersecurity—Gartner Information Technology Glossary. (n.d.). Gartner. Retrieved December 2, 2020, from https://www.gartner.com/en/information-technology/glossary/cybersecurity

Error. (n.d.). Retrieved December 3, 2020, from https://www.inderscienceonline.com/doi/abs/10.1504/IJFSM.2020.111105

Glaspie H.W., Karwowski W. (2018) Human Factors in Information Security Culture: A Literature Review. In: Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_25

Gong, N., & Philbin, G. (2016). *FRAMES OF MIND: CULTIVATING KNOWLEDGE AND CYBERSECURITY*. *17*, 11.

GSMA., 2016. The Mobile Economy: Middle East and North Africa 2016, GSMA Intelligence, pp. 1–70

GSMA_Cybersecurity_A-Governance-framework-for-mobile-money-providers_ Google Scholar

Harris, A., Goodman, S., & Traynor, P. (2012). Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, *8*, 245.

http://erepository.uonbi.ac.ke/bitstream/handle/11295/104304/Final%20version%20LLM%20thesis%20Aug%202018..pdf?sequence=1 Google Scholar

Janine Aron, Mobile Money and the Economy: A Review of the Evidence, *The World Bank Research Observer*, Volume 33, Issue 2, August 2018, Pages 135–188, https://doi.org/10.1093/wbro/lky001

Jilcha, K. (2019). *Research Design and Methodology* (p. 27). https://doi.org/10.5772/intechopen.85731

KenyaCyberSecurityReport2020.pdf. (n.d.-a). Retrieved December 3, 2020, from https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

KenyaCyberSecurityReport2020.pdf. (n.d.-b). Retrieved December 3, 2020, from https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

KenyaCyberSecurityReport2020.pdf. (n.d.-c). Retrieved December 3, 2020, from https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf

Kitime, E. (2018). *A framework of cybersecurity risks on mobile money users in Tanzania: A case study of Dodoma city*. http://repository.udom.ac.tz/handle/20.500.12661/893

Mobilemoneydefinitionsnomarks56.pdf. (n.d.). Retrieved December 2, 2020, from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilemoneydefinitionsnomarks56.pdf

Moturi, C., & Ogoti, G. (2020). Strengthening technology risk management in mobile money lending. *International Journal of Financial Services Management*, *10*(3), 217. https://doi.org/10.1504/IJFSM.2020.111105

NATIONAL CYBERSECURITY STRATEGY.pdf. (n.d.). Retrieved December 2, 2020, from https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf

PECB. (n.d.). *Key Steps for an Effective ISO 27001 Risk Assessment and Treatment*. Retrieved December 3, 2020, from https://pecb.com/article/key-steps-for-an-effective-iso-27001-risk-assessment-and-treatment

SACCO CYBERSECURITY REPORT 2018. Demystifying Cybersecurity for SACCOs, Serianu, 2019

Shrier, D., Canale, G., & Pentland, A. (2016a). *Mobile Money & Payments: Technology Trends*. 26.

Shrier, D., Canale, G., & Pentland, A. (2016b). *Mobile Money & Payments: Technology Trends*. 26.

Sometimes, Cyberattackers Are Going to Get In: The State of Cybersecurity 2018. (n.d.). ISACA. Retrieved December 3, 2020, from https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/sometimes-cyberattackers-are-going-to-get-in-the-state-of-cybersecurity-2018

The Impact Of Mobile Banking On Transaction Costs Of Microfinance Institutions: A Survey Of Microfinance Institutions In Nairobi /57

Wadada, R. (2019). *Journal on Mobile Money*. *1*, 26, 27, 28.

APPENDIX

QUESTIONNAIRE

Guidelines

Kindly take a close to 3 minutes to respond to this questionnaire which is the survey on Cybersecurity Readiness for Mobile Banking among SACCOs: A case of Deposit Taking SACCOs DTS in Nairobi City County in Kenya. Unless otherwise, please use the provided options area(s)

PART A. About Respondent

1. Select your gender?

Male [ ] Female [ ]

2. What is your age range in years?
   A. 19 to 25 [ ]
   B. 26 to 35 [ ]
   C. 36 t0 45 [ ]
   D. 45 and above [ ]

3. What is your highest educational level?
   i. Certificate [ ]
   ii. Diploma [ ]
   iii. Undergraduate degree [ ]
   iv. Postgraduate degree [ ]

4. What role do you play in your SACCO?
   i. Senior personnel responsible for cybersecurity matters [ ]
   ii. ICT head department [ ]
   iii. Technical ICT staff [ ]
   iv. General user of ICTs [ ]

5. How many years have you worked with the SACCO?
   i. 0 to 1 [ ]
   ii. 2 to 3 [ ]
   iii. 4 to 5 [ ]
   iv. above 5 years [ ]

6. Do you think mobile money cybersecurity in your SACCO has been affected by the below strategies?

	Strategy	**SA**	**A**	**N**	**D**	**SD**
1	SACCO governance contribute to cybersecurity resilience					
2	Cybersecurity policies cover Mobile Banking					
3	Cybersecurity training and awareness programs					
4	Compliance with cybersecurity Legal and regulatory requirements					
5	Continuous monitoring and audits of mobile money cybersecurity					

PART B: Identify and Review the Mobile money Frameworks in Place

Do you agree with the following regarding Mobile Money Cybersecurity Readiness in your SACCO?

No	General Information About Cybersecurity Mobile Banking	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Implementation of an effective mobile Banking cybersecurity readiness will reduce loss of resources in our SACCO.					
2	Inadequate governance support and involvement to Mobile Banking cybersecurity program prevent implementation of adequate mobile money Cybersecurity readiness in our SACCO.					
3	Absence of cybersecurity policies adversely affects efforts towards achieving adequate Mobile Money Cybersecurity Readiness in our SACCO.					
4	Staff receive inadequate skills, training, and awareness programs on Mobile Money cybersecurity has result to inadequate Mobile Money cybersecurity in our SACCO.					
5	Lack of training and awareness to SACCO members on Secure mobile banking result in inadequate Mobile Money Cybersecurity Readiness					
6	Premature automation technology levels adversely result in inadequate Mobile Money Cybersecurity Readiness in our SACCO.					
7	Nonexistence of audit and monitoring activities on cybersecurity of Mobile Banking has led to inadequate Mobile Money Cybersecurity Readiness in our SACCO.					
8	Inadequate Laws and regulations in the country influences negativelyon implementation of adequate mobile money Cybersecurity readiness in our SACCO.					

Part C: Adequate Mobile money Cybersecurity Readiness Questions

No	**Adequate Mobile Money Cybersecurity Readiness**	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	There exist appropriate cybersecurity products like cybersecurity technologies (Hardware and Software) Firewall, access control system, Scanners and visual personnel security in our SACCO.					

2	There are presence of automated technologies for the SACCO such us Integration Mobile Money payments activities in our SACCO					
3	Staff possess the certifications and adequate mobile money Cybersecurity skills in our SACCO.					
4	SACCO members are aware of the risk associated with Mobile money services					
5	Cybersecurity availability is one of the desired cybersecurity values for our SACCO.					
6	I view Mobile Money Cybersecurity activities in our SACCO as NOT an overhead activity to my daily work routine.					
7	If you had a cybersecurity threat, are you likely to be aware.					
8	I clearly understand my roles & responsibilities relating tocybersecurity.					
9	My employer understands my roles & responsibilities relating tocybersecurity.					
10	I understand the following policy topics as covered by theICT/cybersecurity policy? I. Password II. E-mail III. Message V. Virus, worms or malicious code V. Two Factor Authentication 2FA VI. Backup VII. IoT					
	SACCO Governance Support to Cybersecurity resilience	**Strongly Disagre**	**Disagree**	**Neutral**	**Agree**	**Strongl vAgree**
1	SACCO Governance commit adequate funds for cybersecurity activities					

2	Top management gives strong and consistent support towardsadoption of adequate cybersecurity practices					
3	Top management regularly receive reporting on the status ofcybersecurity status.					
4	The Board of management has the sub-committee that frequently meet to deliberate on mobile money cybersecurity operations.					
	Mobile Money Cyber**security Policies**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	There are documented mobile money cybersecurity policies and guidelinesthat serves as a basis to inform shared cybersecurity and beliefs values.					
2	Employees are aware, understand and accept ICT/Cybersecuritypolicy rules and guidelines.					
3	Users of ICT systems including mobile services abide by ICT/cybersecurity policies.					
4	The ICT policy including cybersecurity for mobile money is regularly revised or updated.					
	Cybersecurity skills training and awareness programs	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	New employees are offered cybersecurity awareness programme in cybersecurity issues.					
2	Employees frequently receive training on mobile money cybersecurity that informs them on cybersecurity issues and consequences of cyber abuses.					
3	The cybersecurity training programs are customized to individual awareness, technical difficulty or departmental risk profile.					
4	Employees in our SACCO know and understand mobile money cybersecurity and other cybersecurity best practices and their application on real live situation.					

	Legal and regulatory Compliance with cybersecurity requirements	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	There are not enough Government and industry cybersecurityregulations in Kenya					
2	Employee in our SACCO signs information security non- disclosure agreement during each new employee on boarding process.					
3	Cybersecurity regulations and practices are adhered to in our SACCO.					
	Proactive mobile money Monitoring and Audit	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Our SACCO routinely conduct mobile money cybersecurity audit and maintain data of cybersecurity vulnerability and intrusion attempts.					
2	There is mechanism to ensure effective monitoring of cybersecurity systems.					
3	There is mechanism in place to ensure effective monitoring of user violation of ICT/cybersecurity policies.					
4	The management is responsive towards monitoring and control comments and enforce agreed audit recommendations.					