UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

OUTCOME OF TECHNIQUES EMPLOYED FOR CYBER RESILIENCY BY COMMERCIAL BANKS IN KENYA

Research Project

BY

JUDITH NTHENYA KASANGA

P54/34331/2019

Supervisor: Dr. Evans Miriti

August 2021

Submitted in partial fulfillment of the Requirements for the award of MSc. in Information Technology Management Degree.

DECLARATION

This project is my own work and has not been previously presented for an award.

Sign: ______________________________ Date: 26-08-2021

Judith Nthenya Kasanga

P54/34331/2019.

This project has been submitted for an award of Master's degree at the University of Nairobi with my consent as supervisor.

Sign: ______________________________ Date: 26-08-2021

Dr. Evans Miriti

DEDICATION

To my family,

for the encouragement to pursue education to the highest.

To my sisters Shirleen and Wendy, as an inspiration to you.

ACKNOWLDGEMENT

I am grateful to God for the wellbeing and good health that were necessary for completion of this report.

Special thanks go to my family for the encouragement as well as support throughout my years of study. They have been an inspiration and have taught me the essence of hard work.

I appreciate all my colleagues and friends for their continuous support.

I am grateful to my supervisor Dr Evans Miriti for his invaluable guidance as well as encouragement.

I am as well indebted to the other panelists for the constructive critique and valuable contribution that helped in shaping this project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

CBK:	Central Bank of Kenya
CCoA:	Cyber Courses of Actions
SoS:	System of Systems
EU:	European Union
ICT:	Information and Communication Technology
PSPs:	Payment Service Providers
SACCOs:	Savings and Credit Cooperatives
SSA:	Sub-Saharan Africa
SWIFT:	Society for Worldwide Interbank Financial Telecommunication

ABSTRACT

In financial institutions, cyber-attacks have become an inevitable digital hazard that cannot be completely eliminated. Cyber-attacks lead to loss of money among clients leading to discussion and may also lead to inefficient service delivery thus inconveniencing customers. In response to the increasing cyber-attacks, commercial banks are complementing their cyber-security posture with cyber resilience in order to maintain operations in face of adversarial activity. The purpose of carrying out this research was to assess influence of cyber resilience techniques on cyber resiliency in Kenyan commercial banks. Moreover, the study also sought to identify techniques adopted by Kenyan commercial banks; establish the relationship between techniques adopted and level of cyber resiliency in commercial banks in Kenya; and recommend methods to improve cyber resiliency for commercial banks. An explanatory research design was employed as well as target population of 39 departmental heads cybercrime in Commercial Banks situated in Kenya. Census approach was as well deployed in the study and hence all the heads of cybercrime departments in Kenyan Commercial Banks were included in the research. This researcher employed primary and also secondary data. A data collection sheet was utilized to acquire data on the secondary data from annual reports of Kenyan commercial banks. The study utilized semi-structured questionnaires to obtain data from employees working in information and communication technology, cyber security, operations and risk departments. Semi structured questionnaire was used for generation of qualitative and also quantitative data. Additionally, thematic analysis was employed for qualitative data analysis and the results were then presented in form of a narrative. Inferential and also descriptive statistics were utilized for analyzing quantitative data with the support of SPSS version 22. Descriptive statistics in this study comprised of frequency distribution, mean, percentages as well as standard deviation. Additionally, inferential statistics including multivariate regression and also correlation analysis then followed. Tables and figures (pie charts and bar charts) were employed to present the results. Correlation and regression analysis were deployed to assess the association between variables. Moreover, the study found that commercial banks in Kenya had adopted privilege restriction, coordinated protection, dynamic positioning, substantiated integrity, analytical monitoring and dynamic representation to a great extent. However, deception as a cyber resilience technique had been adopted to a moderate extent. Moreover, the study discovered that cyber resilience methods including analytic monitoring, adaptive response, coordinated protection, dynamic representation, dynamic positioning, privilege restriction and substantiated integrity had significant and positive effect on cyber resilience in Kenyan commercial banks. Additionally, deception has insignificant influence on cyber resilience of Kenyan commercial banks. Moreover, this study therefore recommends that the Kenyan commercial banks ought to adopt deception technology to cause adversaries misdirect or waste their resources, delay the effect of attack and confuse and mislead adversaries. Moreover, commercial banks ought to use analytic monitoring to gather, analyse and utilize data to identify vulnerabilities as well as utilize malware and forensic analysis to assess the actual damage by cyber-attacks.

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Significant role is played by commercial banks in a country's financial system and in the national economy. They act as financial intermediaries between a saver who deposits funds in a bank and a borrower who obtains a loan from that bank (Manyange, Adeline & Nyabuga, 2016). They also provide specialized financial services that enable the smooth running of other sectors of the economy in a country. As such, efficient service delivery in commercial banks is important not only to their profitability, but also to the performance of the other sectors of the economy (Nyiranzabamwita & Harelimana, 2019). According to Rasphus (2020), quality service delivery in commercial banks encompasses efficiency, cost effectiveness and convenience, which leads to customer satisfaction. To improve service delivery, commercial banks have adopted technological innovations or digital channels for example agency banking, internet banking and credit cards, debit cards, prepaid cards among others.

In the last one decade, consumers have increasingly been adopting cashless payments via digital channels to make transactions (Nyawanga, 2015). However, while commercial banks have heavily invested in the use of mobile and web-based solutions to enable customers make transactions without necessarily visiting the bank branches, these channels also create new vulnerabilities that commercial banks must look at. In software applications vulnerabilities are deliberately sought after in order to build malware that allows unauthorized access as well as modification, jeopardizing the integrity, accessibility, and confidentiality of ICT systems and networks.

Cyber-attacks targeting commercial banks have greatly evolved in the last one decade due to their growing sophistication, frequency and severity. Despite the excellent level of cyber security protections most commercial banks have set up for themselves the rate of cyber-attacks continues to rise, highlighting their inevitability as well as impossibility of completely securing integrity of financial systems in commercial banks. Security Intelligence Solutions (2020) indicates that more than 50% of the commercial banks in world have experienced at least one form of cyber-attack. The annual Cybersecurity Ventures (2019) report predicts that cybercrime will cost world in excess of $6 trillion every year by 2021, up from $3 trillion in 2015. The rising trend of cybercrime has led to increased worldwide expenditure on information security predicted to hit $123.8 billion in 2020 (Gartner, 2020). In 2016, hackers obtained the credentials of an employee at Bangladesh Bank, the country's central bank, and installed six types of malware on its IT system. The hackers then used the access they had gained to the SWIFT system to disseminate payment requests with $18 billion to Bangladesh Bank's account.

According to Serianu (2017), African businesses Cyber-attacks cost $3.5 Billion in 2017. Nigeria was leading with estimated cybercrime costs of $649 Million. Kenya was second with estimated cost of $210 Million. The report also states that cyber security breaches will continue to outpace the spending and will evolve faster than enterprise security. Odonkor (2020) indicates that an assessment of cyber-security environment of one hundred and forty eight banks in SSA suggests that malware is responsible for 24 percent of all cybercrimes; credit card fraud and phishing account for 30 percent as well as one-third of all cybercrimes, respectively. Despite the fact that 85 percent of banks have witnessed cyber-attacks, all these banks assert to invest $541,102 in network security devices to combat cybercrime each year.

In 2018, cyber-attacks cost the Kenya economy an estimated 29.5 billion shillings. The most affected industries were SACCOs, government entities, banking institutions, betting firms and financial service integrators (Africa Cyber Security Report, 2020). Therefore, the financial services sector was the worst hit sector, with 18 percent of attacks targeting banks, and 10 percent aimed at payment systems. Of the Sh. 29.5 billion lost, Sh. 8.85 billion was from direct costs, while Sh. 20.65 billion was lost indirectly. The costs were incurred as a result of computer compromise, email and phishing scams, attacks on transaction channels, and identity theft. The report also adds that less than a third (29%) of the total amount lost was recovered and 72% of the affected institutions did not report cybercrime to the authorities. Many corporate organizations and governments have realized that despite huge investments in cyber-security defenses, cybercrime incidents are still increasing in frequency and in sophistication.

Cyber resilience is the ability to plan, absorb, recover, and adapt to unfavorable events, and is becoming among the most widely used by a variety of organizations. (Bodeau & Graubart, 2017). Hirsch (2021) argues that resilience is the systems' capability to foresee and adapt to possibility of surprise as well as loss, and has been linked to shift in secure paradigm recognizing the importance of system coping when mitigation is impossible. Creado and Ramteke (2020) indicates that the ability to foresee, withstand, retrieve from, and adjust to unfavorable situations, stresses, compromises or attacks on cyber resources is referred to as cyber resiliency. Cyber resiliency is a system-of-systems or a systems' emergent property (when meaning obviously cyber-attacks among aspects of adversity with which the system ought to be particularly resilient) (Parn & Edwards, 2019).

Cyber-resilience is a compelling complementary alternative to the current cyber-security paradigm (Mileski, Clott & Galvao, 2018). Resilience is the ability of an organization to continue being inexistence or to remain less or more stable in the face of shock or scarcity of resources or from physical threat (Ghadge, Caldwell & Wilding, 2019). Cyber resilience therefore means the ability to consistently deliver the desired outcome in the face of adverse cyberattacks. Resilience has long and illustrious history in a variety of scientific fields, including engineering as well as disaster management. One of its primary advantages is that it facilitates complex organizations to start preparing for adverse events and continue to operate under extremely difficult conditions. Colicchia, Creazza and Menachof (2019) contend that no amount of cyber-security will prevent cyber-attacks. That inevitability of cyber incidents is pushing organizations to focus on how to reduce their impact while remaining in operation. This is the essence of adopting and deepening cyber-resilience.

The Communications Authority of Kenya has pushed through legislations for Cyber-crime including: KICA Act, 1998 and Kenya Information and Communications (Cyber security) Regulations, 2016 and the recent Computer Misuse and Cybercrimes Act 5 of 2018. The central Bank of Kenya has been enforcing incident monitoring and cyber-security and incident monitoring as per the regulatory note (CBK, 2017). Outside Kenya, the Asia Bankers Association declared that cyber-resilience is the future of cyber-security (Asia Bankers Association, 2019). The European Union (EU)also, recognizing the essence of cyber-resilience as a pillar for economic development, stable societies and secure defenses launched the Cyber Resilience for Development (Cyber4Dev) encompassing four countries in Asia and Africa (EU, 2017, 2019).

The cyber security as well as resilience concepts differ. Moreover, cyber security focuses on limiting access of data to minimize disclosing information into risk (Panda & Bower, 2020). The notions of resilience and cyber security and resilience are not the same. Because cyber security refers to the procedures as well as measures used to keep computer systems and information safe, it tends to focus on restricting accessibility of data to reduce possible risk (Panda & Bower, 2020). Cyber resilience refers to cyber-ability system's to effectively perform in the face of business-environmental threats (Colicchia, Creazza & Menachof, 2019).

Many corporate organizations and governments have realized that despite huge investments in cyber-security defenses, cybercrime incidents continue to increase in frequency and sophistication. This concern has reached a critical level in Kenya, specifically among banks. In view of the great value attached to Cyber resilience in the modern organizations, this study seeks to establish the cyber resilience techniques adopted by Kenyan banks and their effect on cyber resilience.

A cyber resiliency approach is a collection of technologies as well as processes designed to accomplish one or more of the goals established during prioritization process. Ross, Graubart and Bodeau (2018) indicates that cyber resilience techniques include adaptive response, coordinated protection, analytic monitoring, deception, dynamic positioning, diversity, dynamic representation, realignment, redundancy, privilege constraint, segmentation and substantiated integrity. Adaptive Response involves optimization of the capability to respond in appropriate and timely manner (Bodeau & Graubart, 2017). In addition, analytic monitoring encompasses monitoring and detecting adverse conditions and actions in timely conditions as well as actionable manner (Hausken, 2020). While coordinated Protection involves implementation of defense deep strategy in order for adversaries so as to overcome numerous barriers, deception involves misleading, confusing and hiding essential assets. Moreover, cyber resilience technique uses heterogeneity to reduce mode failures, especially attacks that take advantage of common vulnerabilities (Ross, Graubart & Bodeau, 2018).

Privilege restriction not only involves restricting privileges depending on the user and also system attributes but also environmental factors.

1.2 Statement of the Problem

Cyber-attacks have now become an unavoidable digital risk that even the most sophisticated financial institutions will never be able to fully eliminate, no regardless of how much money they invest in cutting-edge security technology (Hausken, 2020). If a cyber incident jeopardizes the availability, confidentiality or integrity of data, it can cause panic and cascading effects that result in financial system instability (Borum, Felker & Feyes, 2015). In addition, cyber-attacks lead to loss of money among clients leading to discussion and may also lead to inefficient service delivery thus inconveniencing customers (Kosutic & Pigni, 2020). In response to the increasing cyber-attacks, commercial banks are bolstering their cyber-security posture with cyber resilience in order to keep operations running in the face of adversarial activity.

According to Ngugi (2019), financial institutions operating in Kenya have become a popular target for cybercriminals, with records indicating that in 2016 they lost approximately Sh17 billion to fraudsters, an increase from Sh14 billion in the previous year. In addition, Olingo (2018) indicated that in a month, two Kenyan banks lose $0.86 million to hackers. Cybercrime leads to panic among customers, which in turn affects the utilization of digital channels in making transactions. In addition, it disrupts service delivery and inconveniences the customers as it leads to inefficiency and at times total inaccessibility of services (Leonard, Ogara & Liyala, 2020).

Therefore, in recent times, the extreme uncertainty, uncertainty, and dynamic changes of potential cyber threats have rendered risk assessment efforts incapable of adequately addressing cyber-security issues for critical infrastructures (Hausken, 2020). Majority of researches in field of cyber resilience focus on technical qualities, with only a few studies looking into organizational aspects of cyber resilience (Odhiambo, 2018; Njoroge, 2020). However, cyber resilience entails technical as well as organizational elements (Olingo, 2018). Rather than simply implementing cyber security controls, organizations must take a resilience method to cyber security.

Various researches have been performed on cyber security and cyber resilience in Kenya. For instance, Mayunga (2019) conducted a study on developing and assessing a cyber-resilience framework for Kenyan Banks; Odhiambo (2018) examined the effect of cyber securities strategies on implementation of online banking in Commercial Banks in Kenya; and Njoroge (2020) studied whether cybercrime-linked costs influences the growth of accounting innovation products as well as services at the National Commercial Bank of Kenya. However, these studies did not show how adoption of cyber resilience techniques influences cyber resilience in Kenyan commercial banks.

1.3 Purpose of study

The purpose of carrying out this research was to examine influence of cyber resilience techniques on cyber resiliency in commercial banks in Kenya

1.4 Objectives of the Study

Objectives of this study were;

i. To evaluate techniques adopted by commercial banks in Kenya

ii. To assess the relationship between techniques adopted and the level of cyber resiliency in commercial banks in Kenya

iii. To recommend methods to improve cyber resiliency for commercial banks

1.5 Research Questions

This study was anchored on below questions;

i. What techniques have commercial banks implemented to improve cyber resiliency?

ii. What is the effect of cyber resilience techniques implemented on level of cyber resiliency in commercial banks in Kenya?

iii. How can cyber resiliency in Kenyan commercial banks be improved?

1.6 Significance of the Study

Management of Kenyan commercial banks, policy makers, Kenyan government and also academicians and researchers may benefit from this research. To the management of Kenyan commercial banks, the study provides information on cyber resilience techniques and service delivery in commercial banks in Kenya. Specifically, the research identifies the cyber resilience techniques used by commercial banks and how they affect cyber resilience. This information is used to develop strategies to address cybercrime in commercial banks so as to improve cyber resilience.

Commercial banks play a fundamental role in national economy as they act as financial intermediaries between individuals saving in banks and borrowers. Therefore, the findings of this study are of great importance to the Kenyan government and policy makers in Kenya as it provides information on the influence of cyber resilience techniques on cyber resilience that can be used to formulate and implement policies to address cyber-attacks and cyber-crime related to commercial banks. The government of Kenya may also be in a position to review or develop new policies to protect customers, who include players in different sectors in the economy, from losing their money.

The study adds information to existing body of knowledge pertaining to influence of cyber resilience techniques on cyber resilience in Kenyan commercial banks. To other scholars, researchers and also academicians, findings provides essential information that may be utilized as research material as well as in the identification of research gaps in studies related to cyber resilience techniques. The study forms basis upon which further researches can be performed on influence of cyber resilience techniques on cyber resiliency in other sectors of the economy.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature on an overview of cyber security, trend of cyber resilience, cyber resiliency, theoretical review, empirical review, conceptual framework presenting hypothesized association between variables and summary of the literature.

2.2 Cyber Resilience in Commercial Banks

Resilience is defined broadly as “a system's ability to avoid disruption and reorganize whilst also undergoing change so as to retain similar function, personality, structure, as well as feedbacks" (Omar & Kilika) (2018). It is a multidisciplinary concept that focuses on a complex, adaptive, nonlinear system's dynamic ability to self-repair in response to trauma or transition to the recent stable equilibrium. The globally integrated financial system's proclivity to oscillate from one crisis to the next makes resiliency a critical concept for financial system (Manyange & Atuhairwe, 2016). Since the financial crisis, this term has appeared frequently in regulatory and also supervisory discourse as well as documents.

The notion of cyber-resilience is an appealing complement ‘forecast and protect' technique that has overtaken security for all information for several decades (Chesaina & Gitonga, 2019). Confronted with bleak reality that no digital system can guarantee impregnability in the face of increasing assaults, organizations are trying to come to terms with the need to design technologies and processes that provide assistance following catastrophic attacks (Farayibi, 2016). To borrow a powerful metaphor, organizations must learn to survive on a diet of poisoned fruit once they admit that they operate in a constant state of cyber-vulnerability while reaping significant productivity benefits from the technologies that also threaten their survival.

In a study on the application of cyber-resilience in financial institutions, Dupont (2019) indicates that in financial institutions cyber-crime involves capacity to retrieve from, withstand and adapt to external upsets resulting from cyber risks. Its main advantage is that it allows complex organizations to start preparing for adverse events and continue to operate under extremely difficult conditions. However, the current “prevent and protect” paradigm is insufficient, and a cyber-resilience orientation must be combined to risk managers' toolbox. The world Economic Forum (2019) indicates that effective cyber resilience reduces the impact of cyber-attacks on commercial operations in commercial banks, FinTech companies and other financial institutions, lowers frequency as well as level of loss to clients and is critical to preserving consumer trust in the financial system as a whole.

2.3 Cyber Security to Cyber Resilience

Collier, Walters & DiMase, (2014) defines cyber security as the technologies, measures and also processes that are intended to safeguard data, systems and also networks from cybercrime. Cyber-attack risk and entities, individuals and organizations are protected cyber security, from intentional exploitation of networks, systems and also technologies. Moreover, it has a broader scope that includes cyber security as well as business resilience. Moreover, cyber security is beneficial devoid of compromising functionality, and there is solid business continuity plan in place to continue with operations in case cyber-attack is successful (Hollnagel, Woods & Leveson, 2006).

Cyber resilience enables businesses to acknowledge that hackers have added benefit of innovative devices, the aspect of surprise, the target, as well as the ability to succeed in their attempt. This concept assists businesses in preparing for, preventing, responding to, and recovering to desired secure condition (Kott, Ludwig & Lange, 2017). This represents cultural shift in which an organization views security as all-time job and incorporates security practices into daily operations. In relation to cyber security, cyber resilience necessitates a shift in thinking and a more agile approach to dealing with attacks.

A cyber resilience framework, also known as a cyber security framework, is an essential modern business component. In face of increasing malware, phishing, as well as high-tech threat actors, cyber-resilient firm can place itself as secure model for protection of data that clients can rely on (Kott & Abdelzaher, 2014). Considering the increasing security risks associated with remote working, numerous businesses remain unprepared (Connelly, Allen & Linkov, 2017). It is not enough to have the best incident response tools to develop cyber resilience.

2.4 Cyber Resilience Techniques

Cyber resilience is an organization's ability to prepare for, respond to, and also recover from cyber-attacks. Moreover, an organization has cyber resilience if it can defend itself against such attacks, mitigate the effects of a security incident, and ensure the continuity of its operations both during and after the attacks (Linkov, 2018). Organizations are beginning to incorporate cyber resilience into their cyber-security strategies. While cyber-primary security's goal is to protect information technology and systems, cyber resilience is much more responsible in ensuring that business is delivered. Furthermore, the preferred result is business delivery, which emphasizes on business goals over IT system requirements (Collier, Walters & DiMase, 2014).

Each method is distinguished by the particular capabilities it gives as well as intended outcomes of utilizing technologies/processes it incorporates (Hollnagel, Woods & Leveson, 2006). The cyber resiliency methods convey understanding of threats and also technologies, processes as well as concepts associated with boosting cyber resiliency in order to address threats. Framework for cyber resiliency engineering supposes that cyber resiliency approaches will be applied selectively to design or architecture or even business functions to organizational mission together with their supporting system resources (Linkov, 2018). Because there are natural synergies as well as conflicts among cyber resiliency methods, engineering trade-offs should be made. Moreover, cyber resiliency methods are anticipated to evolve over time with evolving threats, security practices, new ideas arise and research advances are as well made,.

2.4.1 Adaptive Response

Adaptive Response method enables systems as well as firms to respond accordingly and also dynamically to particular situations, utilizing agile as well as another possible operational contingencies so as to maintain lowest operational capacity, limiting consequences and also avoiding destabilization, and taking preventative action where suitable (Connelly, Allen & Linkov, 2017). Adaptive Response entails selecting, carrying out, and assessing the implementation of the CoA that alters attack surface, retains essential capabilities, and also restores functional capacities. Dynamic Reconfiguration and Composability, Dynamic

Allocation of Resources, as well as Preemptive Action are examples of capabilities that support Adaptive Response. The capabilities can be executed by constituents systems in a SoS, either with intervention of administrator or operator or through pre-defined automated contingencies response. It improves the ability to respond to unfavorable situations, stresses, or attacks, or indicators of these, in a timely and appropriate manner, maximizing ability to sustain business operations, lower consequences as well as avoid destabilization (Kott & Abdelzaher, 2014).

Adaptive Response entails deploying cyber courses of action (CCoA) to respond dynamically to particular situations, employing agile as well as alternative operational scenarios in order to sustain the lowest operational capabilities, avoid destabilization and limit consequences,. CCoA entails putting in place pre-determined measures to help minimize as well as manage risks (Kott, Ludwig & Lange, 2017). Adaptive Response improves an organization's ability to respond to changing adversary activities in a timely and appropriate manner, maximizing its ability to maintain the integrity and also availability of essential services. Dynamic Reconfiguration and Resource Allocation, and Dynamic Composability are three approaches to using Adaptive Response.

2.4.2 Analytic Monitoring

Analytic Monitoring methods constantly obtain, fuse, and also analyze data to utilize threat intelligence, find potential unfavorable conditions indications, identify vulnerabilities and possible or actual damage. Damage Assessment and Monitoring, Sensor Fusion as well as Analysis, and Forensic and Malware Analysis are the Capabilities that support Analytic Monitoring (Linkov, 2018). It improves the capability of detecting possible unfavorable conditions, revealing the degree of unfavorable situations, attacks, and identifying actual or potential damage. Moreover, it provides the information required for situational awareness.

2.4.3 Coordinated Protection

Coordination of multiple and diverse methods to safeguard fundamental resources throughout the subsystems, systems, layers as well as organizations is the goal of coordinated defense techniques (Woodard, 2019). Technical Defense-in-Depth is a key approach, and capabilities supporting Coordinated Defense entail Consistency and Coordination Analysis, as well as Adaptive Management (Connelly, Allen & Linkov, 2017). It is necessary for adversary to circumvent numerous safeguards (execute defense-in-depth strategy). Coordinated defense makes it hard for an adversary to launch an attack on important resources, increasing adversary's cost and increasing chances of adversary detection. They make sure that usage of specific safety method does not have negative effects by trying to interfere with other protection method, and they validate cyber plans of action realism

2.4.4 Deception

Deception is about misleading, confusing, hiding or concealing critical assets or exposing to the adversary the covertly tainted assets. Misleads or confuses the adversary, leaving adversary unsure of ways in which to go forward, delaying overall impact of attack, increasing likelihood of being exposed, leading to wastage or misdirect of resources, as well as prematurely uncovering adversary tradecraft (Woodard, 2019).

Deception technology is a novel and cutting-edge approach to addressing the issues that organizations face in today's cyber environment. These platforms can perform deception-based detection at every layer of the network stack, allowing for efficient detection of every threat vector. Deception solutions use high-interaction decoys and lures to effectively trick hackers into revealing themselves, thus also closing the “detection deficit” (Linkov, 2018). Deception technology helps in addressing the key specific problems by allowing an organization to identify complex threats far more rapidly than previously possible, as well as lowering the costs linked with detecting more mundane (less technologically advanced) attacks..

2.4.5 Dynamic Positioning

Dynamic Positioning methods disseminate and dynamically reposition functionality and also assets, altering attack surface. Moreover, functional reposition, Asset Mobility, as well as Distributed Functionality are examples of capabilities. It increases the capability to rapidly recover from non-adversarial events. According to Ganin, Kitsak and Linkov (2017) it impedes adversary's ability to identify, remove, or business assets, or corrupt purpose causing the adversary to expend extra time and also energy in locating critical assets, increasing likelihood of adversary disclosing its actions as well as tradecraft prematurely.

2.4.6 Privilege Restriction

Privilege Restriction methods limit the benefits granted to users and entities, as well as the requirements placed on resources (Connelly, Allen & Linkov, 2017). Privilege Management and Privilege Restrictions Based on Usage are two capabilities. It reduces the impact and likelihood of unintended actions by authorized users compromising information or services. Impose additional time and effort on an adversary in order for them to obtain credentials. It also limits the adversary's ability to fully capitalize on credentials obtained (Connelly, Allen & Linkov, 2017).

2.4.7 Dynamic Representation

Dynamic Representation is the ability to reflect modifications in behavior or state, which manifests itself through the construction and maintenance of a dynamic representation of elements, systems, adversary activities, services, and other unfavorable situations, as well as the effects of various alternatives (including cyber courses of action) (Ganin, Kitsak & Linkov, 2017). Dynamic Representation must first ensure the presence of static representations before expanding on them so that adversary actions, when first detected as well as analyzed, will inform mission situational awareness as well as response.

2.4.8 Substantiated Integrity

Kott, Ludwig & Lange, (2017) suggests that substantiated Integrity methods provide methods for determining if essential services, data stores, data streams, as well as constituents have been ruined. Quality Checks, Behavior Validation and Provenance tracing are some approaches. It facilitates the determination of right result when there are conflicts between various services or inputs. Detect an adversary's attempts to deliver compromised software, hardware or data as well as successful modification or fabrication.

2.5 Theoretical Review

Fraenkel, (2014) suggests that theory refers to a collection of principles that are meant to explain collection of realities or occurrences, particularly that which been tested frequently or is largely acknowledged and also can be utilized to forecast natural occurring phenomena. Theoretical framework explains and also introduces the theory which explains existence of research problem being investigated. The study was anchored on resilience theory and Cyber Resilience Engineering Framework.

2.5.1 Resilience Theory

Resilience theory was developed in the early 1989 (Weick, Rapp, Sullivan & Kisthardt, 1989). In a strength-focused approach, the theory helps in comprehending how some people can recover after in life undergoing adversity. According to resilience theory, factors that characterize resilience and thriving include sense of coherence, strong coping skills, optimism, adaptability, risk-taking, perseverance, high tolerance of uncertainty and determination. From a technological perspective, cyber resilience involves the system's capacity to prepare for, absorb, regain and also adapt to unfavorable effects, mainly those related to cybercrimes (Greene, Galambos & Lee, 2014).

Several studies have used resilience theory to show how organizations develop strategies to ensure resilience even during uncertainties. For instance, Chewning, Lai and Doerfel (2013) conducted a study on organizational resilience and utilization of information and communication technologies and argued that organizations have to come up with ways of preparing, responding and adapting when there are cyber-attacks. In addition, Atwell, Schulte and Westphal (2019) conducted a study linking resilience theory to diffusion of innovations theory in order to understand potential for perennials in U.S. Corn Belt. Further, Ahiauzu and Jaja (2015) utilized the resilience theory to show the relationship between process innovation and organizational resilience in South- Nigerian public universities.

Organizations face unforeseen situations or risk to fail during their lifetime and hence resilience is a desirable trait that is also strategically advantageous (Greene, Galambos & Lee, 2014). Furthermore, firms can consider a variety of standby teams to deals with various unexpected problems to increase resilience, but this will increase their overheads. Building organizational resilience thus becomes a process of balancing costs against potential risks. Costs clearly take a back seat in so-called high-reliability organizations in order to achieve resilience. As Zimmerman (2013) points out, these organizations are preoccupied with failure. As a result, despite much higher costs, organizing operations across resilience makes sense. For business entities that do not encounter the same types of risks, attaining resilience for the sake of achieving resilience is clearly not a viable option. Even though, these companies depend on the resilience of their existing structures and also processes, they primarily operate to fulfill the tasks of manufacturing products as well as serving customers.

Even after experiencing cyber-attacks commercial banks have to bounce back, improve on their security and continue delivering efficient and cost-effective services to their customers. Cyber resilience has a broader scope that includes cyber security as well as business resilience. This concept assists organizations in preparing for, preventing, responding to, and recovering from insecure state. This represents cultural shift in which an organization views security as all-time job and incorporates security practices into daily operations. Cyber resilience In relation to cyber security necessitates a shift in thinking and a more agile approach to dealing with attacks.

2.5.2 Cyber Resilience Engineering Framework (CREF)

CREF is a framework used in the evaluation of an organization’s resiliency (Bodeau, Brtis & Graubart, 2013). The CREF is drawn from taxonomies and frameworks in disciplines of network resilience, resilience engineering, fault tolerant and infrastructures’ systems resilience. While CREF tends to focus on cyber, derivation allows CREF to be widened to also include potential threat sources such as natural occurrences and errors and also adversarial actions such as non-cyber-attack vectors, cyber-physical, and purely cyber systems (Ariful, Sachin, Kimberly & Bheshaj, 2016).

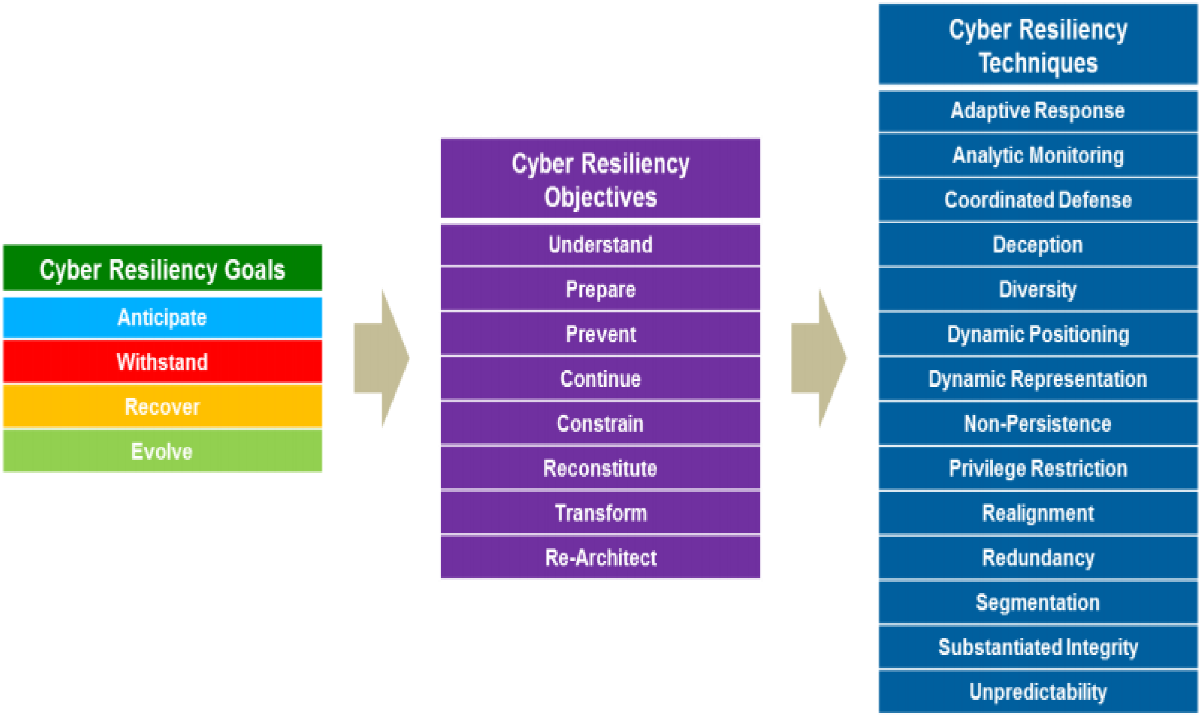


Figure 2. 1: Cyber Resiliency Engineering Framework

Source: Bodeau, Brtis and Graubart (2013)

As shown in Figure 2.1 the CREF is made up of resiliency objectives, goals, and techniques. The goal of cyber resiliency framework, methods and objectives is to plan cyber resiliency. Goals are desired outcomes' high-level statements that aid in scope of the cyber resiliency sphere. Cyber resilience goals include anticipate, withstand, recover and evolve (Bicknell, Heinbockel, Laderman & Serrao, 2017). Objectives are particular statements of expected results, to act as link between goals and techniques. They are usually expressed in a way that facilitates evaluation; it is simple to create questions such as "how quickly" or " well" or with the degree of "trust or confidence" should the objective be accomplished.

Cyber resiliency methods are ways of attaining cyber resiliency goals applied to design or architecture of various business functions or mission and also cyber resources to help them (DiMase, Collier & Heffner, 2015). Methods are applied selectively to a design or architecture of business various functions or mission, as well as the cyber resources to enable them in achieving goals. A particular technique typically aids numerous objectives, however it may be extraordinary to a particular one.

Cyber Resiliency Engineering Framework has been used in studies on cyber security and cyber resilience. For instance, Bicknell *et al.* (2017) used the framework to study the role of cyber resiliency in dealing with supply chain attacks. In addition, Ariful *et al.* (2016) used Cyber Resiliency Engineering Framework in a study on realization of cyber-physical systems, security practices and resilience frameworks. Further, DiMase, Collier and Heffner (2015) utilized the Cyber Resiliency Engineering Framework in a study on systems engineering framework.

2.5.3 Justification of the Choice of Cyber Resiliency Engineering Framework

In Kenya, Mayunga (2019) conducted a study on developing and assessing a cyber-resilience framework for Kenyan Banks. The research used descriptive research approaches augmented by quantitative techniques to measure the variables. The framework was first validated by cyber security subject-matter experts and then through a pilot study. A sample of forty out of the possible forty-four banks in Kenya was selected using simple random sampling. The results indicated that present discourse in cyber security is increasingly encouraging increased emphasis on cyber-resilience. Since an ecosystem is shared by the banks with other organizations, cyber-resilience ought to be given focus by the firms to facilitate cyber-safety at level.

2.6 Empirical Review

In Norway, Hausken (2020) conducted an assessment of cyber resilience in companies and societies. The study used critical review of literature. Results indicated that Cyber resilience is linked to insurance of any cyber via cyber contracts’ preconditions or entry requirements, the importance of different services for example incident response, cover limitations and data gathering. Additionally, cyber resilience is associated with internet of certain things, which can be anticipated to make life simpler in future via artificial intelligence as well as device learning, whilst also remaining endangered due to large surface of attack, inadequate technology, potential high confidence in software and computers, ethics and challenging handling of data.

In a critical review of literature, Dupont (2019) examined significance and applicability of cyber-resilience of financial institutions in Indonesia. The findings indicated that the financial sector's need for cyber-resilience, highlighting the various types of threats that target financial systems as well as the various measures of their negative impact. The findings indicated that the current “prevent as well as protect” paradigm is insufficient, and that cyber-resilience orientation must be added to risk managers' toolbox.

In the United Kingdom, Boyes (2015) examined cyber-security and cyber-resilient supply chains. The research utilized descriptive research approach and discovered that increased use of IT introduces variety of cyber-security risks affecting supply chain cyber-resilience in terms of product or services received by customer and also supply chain operation. Factors such as international markets of technology constituents or software, systems ownership in supply chain, diverse legal jurisdictions involved, and immense third parties usage to produce functionality complicate the situation.

In Nigeria, Jegede and Olowookere (2016) conducted an evaluation of cyber fraud and risks in business environment. The population of the study was financial institutions in Nigeria. The findings indicated that detected risks should be properly addressed to avoid secondary impacts that lead to vulnerabilities interfering with institution's life, as well as well-being of its customers. Aside from installing threat-response technologies, institutions must work to strengthen trust environment. They owe it to their clients to keep them up to date on the existence of actual and potential risks from online environment. Protective actions must be implemented to avoid the compromise of individual information critical to clients' financial and domestic survival, and obtaining consent is critical in this regard, particularly if such requests are made for secondary uses.

2.7 Conceptual Framework

Russell, (2013) suggests that conceptual framework refers to a visual or diagrammatic representation that assists in illustration of anticipated associations between study variables and concepts. Figure 2.1 shows the associations study variables. Independent variables in this study were cyber resilience techniques like adaptive response, analytical monitoring, deception, coordinated protection, privilege restriction, dynamic positioning, substantiated integrity and dynamic representation. The dependent variable was cyber resilience in commercial banks in Kenya.

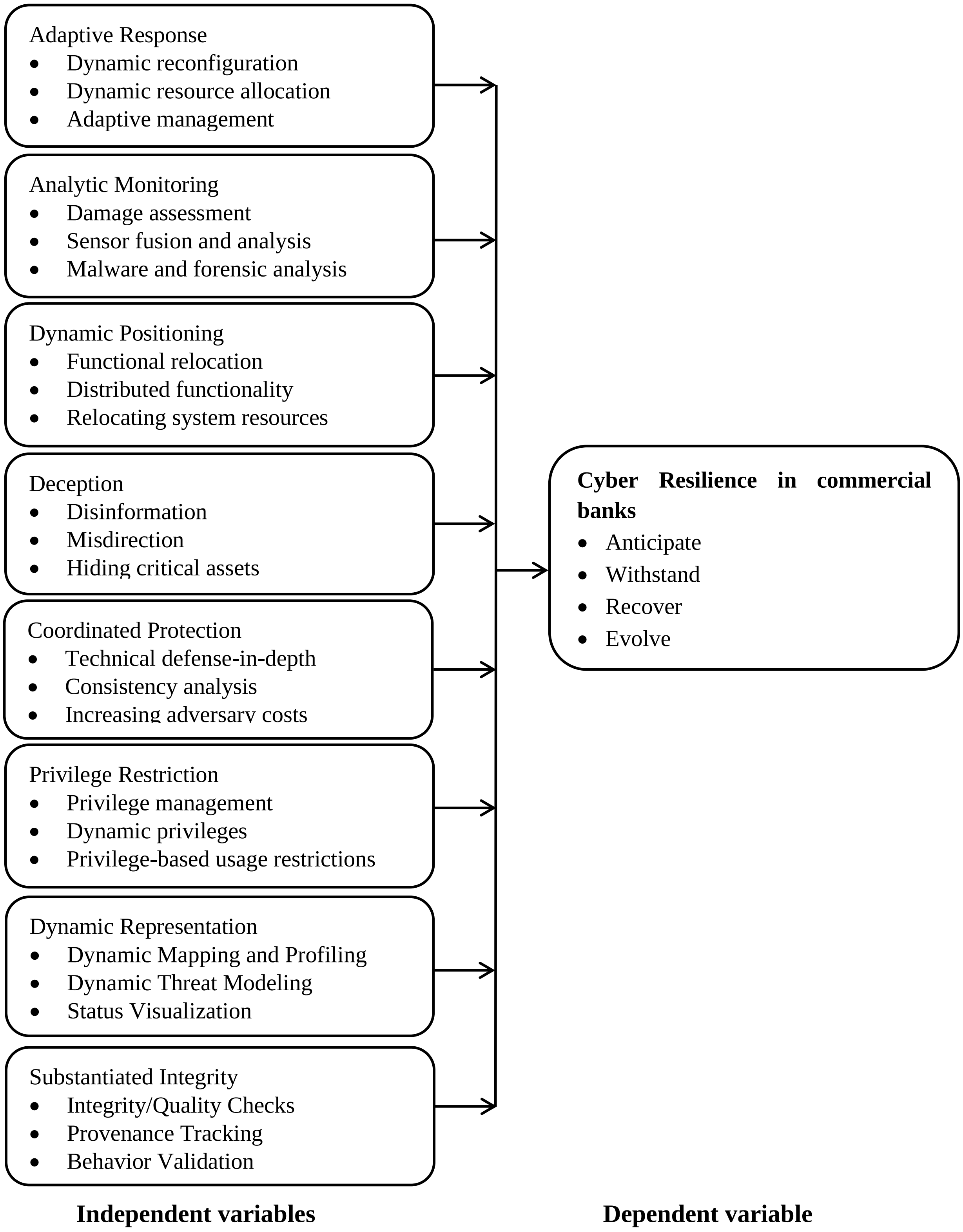


Figure 2. 2: Conceptual Framework

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The term "research methodology" is the process of gathering and analyzing data in order to answer specific research questions. The chapter comprises research design, study population, sample size, sampling frame as well as sampling method, data collection instrument, procedure of data collection, reliability and validity and data analysis and also presentation.

3.2 Research Design

Yevale, (2016) suggests that research design refers to a strategy adopted in integration of diverse aspects of a research coherent and logical way, thus ensuring the research problem is addressed. According to Stokes and Wall (2017), research approach is foundation for gathering, measuring and analysing data. An explanatory research design was deployed by the researcher. This design demonstrates that the study seeks to explain instead of describing the phenomenon under investigation. The design is also referred to as an explanatory research design, and it is used to reveal the extent and nature of the relationships (Russell, 2013). Explanatory research is usually concerned with problem analysis with the goal of determining the sequence of the association between study variables. The researcher evaluated the association between cyber resilience techniques and cyber resilience in Kenyan commercial banks.

3.3 Target Population

The set of events, services or people, group of households or items with similar attributes that a researcher seeks to investigate is what is referred to as target population (Fraenkel, 2014). The unit of analysis is defined as a major entity that a particular researcher analyses in a study (Bhattacherjee, 2012). The unit of analysis was thirty nine Kenyan commercial banks operating. A unit of observation refers to an object about which information is collected (Greenfield & Greener, 2016). The unit of observation in the study was the heads of cyber security in commercial banks. These individuals in the department were selected because they are involved in ensuring cyber security and dealing with the impacts of cybercrime in their financial facilities. The target respondents were therefore 39 departmental heads of cybercrime in Kenyan Commercial Banks.

3.5 Sample Size and Sampling techniques

Given that the study population was relatively small (39), the researcher used census approach to include all members of the population. These included 39 cybercrime departmental heads in Kenyan Commercial Banks. Census method refers to a procedure of enumerating, acquiring, and recording information on members of the study population (Fraenkel, 2014). The statistician gathers data for every unit of the population using the census or complete enumeration method.

3.6 Data Collection Instruments

This study utilized secondary as well primary as data. Moreover, secondary data is defined as the type of data that has earlier been collected as well as analyzed and other researchers can access it. In this study, a data collection sheet was deployed to obtain data on the secondary data from annual reports of commercial banks in Kenya. According to Creswell (2014), Primary data is information gathered from immediate occurrence that has also not been subjected to further processing or manipulation. According to Babbie (2017), qualitative research tools (focus group discussions, observations and interview guides,) and quantitative research instruments can be used to gather primary data (questionnaires). The study utilized questionnaires to obtain data from staff working in information and communication technology, cyber security, operations and risk departments. Moreover, questionnaires included closed-ended as well as open-ended questions. Because they are immediately usable, the questions were deployed to save time as well as money while also facilitating an easier analysis. Open-ended questions were utilized because they normally inspire respondents to provide wide and also felt answers without feeling constrained in disclosing information. According to Adams (2014), a questionnaire is cost-effective method of gathering information, especially from large group of respondents, and it facilitates anonymity. Because some of the information required is sensitive, questionnaires were used in this study to ensure anonymity.

The questionnaire comprised of four main sections. First section obtained general information on each of the participants. Second section obtained information on cyber resilience in commercial banks. The third section obtained information on cyber resilience techniques adopted by commercial banks.

3.8 Pilot Testing

Pilot test refers to a small-scale systematic review aimed to analyze feasibility, duration, unfavorable events, cost and improve research design prior to the execution of the final study (Babbie, 2017). Pilot study was done to evaluate research tools' dependability and validity. Pilot study is designed to eliminate problems that may arise during final survey. The pilot test was conducted in one branch of Kenya Commercial Bank with a pilot group of 11 individuals. According to Fraenkel (2014) 10 percent sample size of total sample size needed for final research should be used. The researcher modified the questions in relation to the feedback from the pilot test and then developed the final questionnaire.

3.8.1 Validity of Research Instruments

Bhattacherjee (2012) argues that the extent to which the findings from the analysis process embody phenomenon being studied is referred to as validity. Validity is classified into two types: content validity as well as face validity. Moreover, face validity is the likelihood that a certain question will either be misunderstood or misinterpreted. Pre-testing, as defined by Fraenkel (2014), is an appropriate way to enhance face validity. Conversely, content validity is normally described as the extent to which given measure depicts social construct aspects. The research tools' content validity was enhanced by soliciting experts' views on subject area, specifically supervisors. Additionally, research tools' face validity was enhanced by performing pilot study as well as modifying questions that are unclear or ambiguous.

3.8.1 Reliability of Research Instruments

In statistics and psychometrics, reliability is a measure's overall consistency. A measure is deemed as reliable if it gives consistent results in consistent conditions (Russell, 2013). Cronbach's alpha coefficient, ranging from 0 to 1, is used to calculate data reliability. Cronbach's alpha measures how directly connected a group of things is. It is scale reliability metric (Stokes & Wall, 2017). Cronbach's alpha in this study was used to determine questionnaire's reliability. Higher alpha coefficient values indicate that the items used to measure the concept of interest are consistent. Cronbach's alpha greater than 0.7 is deemed as acceptable and that below 0.7 is deemed questionable.

Table 3. 1.Reliability Test

Cyber Resilience Techniques	**Cronbach'salpha**	**No. ofitems**	**Comment**
Adaptive response	0.941	3	Acceptable
Analytical monitoring	0.880	2	Acceptable
Coordinated protection	0.720	3	Acceptable
Deception	0.709	3	Acceptable
Dynamic representation	0.929	3	Acceptable
Dynamic positioning	0.887	2	Acceptable
Privilege restriction	0.915	3	Acceptable
Substantiated Integrity	0.795	3	Acceptable

These findings imply that variables had a Cronbach's alpha of above 0.7 and thus research tool was reliable.

3.7 Data Collection Procedure

The researcher obtained a permission letter to collect data from University of Nairobi shortly before the start of data collection. Moreover, research permit was also requested from NACOSTI. The researcher also wrote a letter to the respondents explaining the purpose and the need for collecting data. The researcher conducted daily follow-ups to ensure that the questionnaires were being collected and filled out as expected. This entire data collection process took one month.

3.9 Data Analysis and Presentation

The study utilized semi-structured questionnaire to collect qualitative and quantitative data, which was then analyzed separately using various techniques. Thematic analysis was used to analyze qualitative data. Thematic analysis is a qualitative data analysis technique. It is usually used to describe a group of texts, such as interview transcripts. The researcher carefully examines the data to find common themes – ideas, topics and meaning patterns that appear repeatedly (Yevale, 2016). Thematic analysis involves generating reviewing themes, defining as well as naming themes and writing up.

Analysis of quantitative data was done by utilizing analyzed descriptive and also inferential statistics. Inferential statistics (multivariate regression as well as correlation analysis) then followed. Findings were displayed in tables and figures including pie charts as well as bar charts. Moreover, correlation analysis and also regression analysis was utilized to examine the link between study variables. Multi regression model was;

$$Y = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \beta_7 X_7 + \beta_8 X_8 + \varepsilon$$

Whereby;

Y = Cyber resilience in commercial banks in Kenya
B_0 = Constant
β_1- β_8 =Coefficients
X_1 = Adaptive Response
X_2 = Analytic Monitoring
X_3 = Coordinated Protection
X_4 = Deception
X_5 = Dynamic Positioning
X_6 = Privilege Restriction
X_7 = Dynamic Representation
X_8 = Substantiated Integrity
ε = Error term

CHAPTER FOUR

RESEARCH FINDINGS AND DISCUSSIONS

4.1 Introduction

Data analysis and also the interpretation of findings together with presentation of research findings in line with research objectives are presented in this chapter. The study begins with respondents' response rate, demographic information, followed by extent of adoption of cyber resilience techniques, extent of cybercrimes prevention, relationship between cyber resilience techniques and cyber resilience, cyber resilience descriptive analysis, recommended methods to improve cyber resilience and inferential statistics. Findings were then displayed in both figures and also tables.

4.2 Response Rate

This study sampled 39 of cyber security departmental heads in Commercial Banks in Kenya. Researcher administered 39 research tools among heads of cyber security departments in Commercial Banks in Kenya, out of which 37 of them were filled and also returned. Therefore, 94.87% response rate was obtained. According to Adams (2014), a 75% and above response rate is normally considered reliable. In addition, Bhattacherjee (2012) indicates that above 50% response rate is adequate for data analysis as well as presenting the results, but that above 70 percent is considered as outstanding. Therefore, response rate of 94.87% was within the commended limit.

4.3 Respondents' Demographic Information

Demographic information of the cybercrime departmental heads in Kenyan Commercial Banks comprised of respondents' gender, age bracket, education level as well as duration of working.

4.3.1 Respondents' Gender

Respondents were sked to point out their gender. Findings were depicted in Figure 4.1. According to the study, 79.5 % of the participants were male and 20.5% were female. Moreover, this means that large numbers of the respondents in Commercial Banks are male.

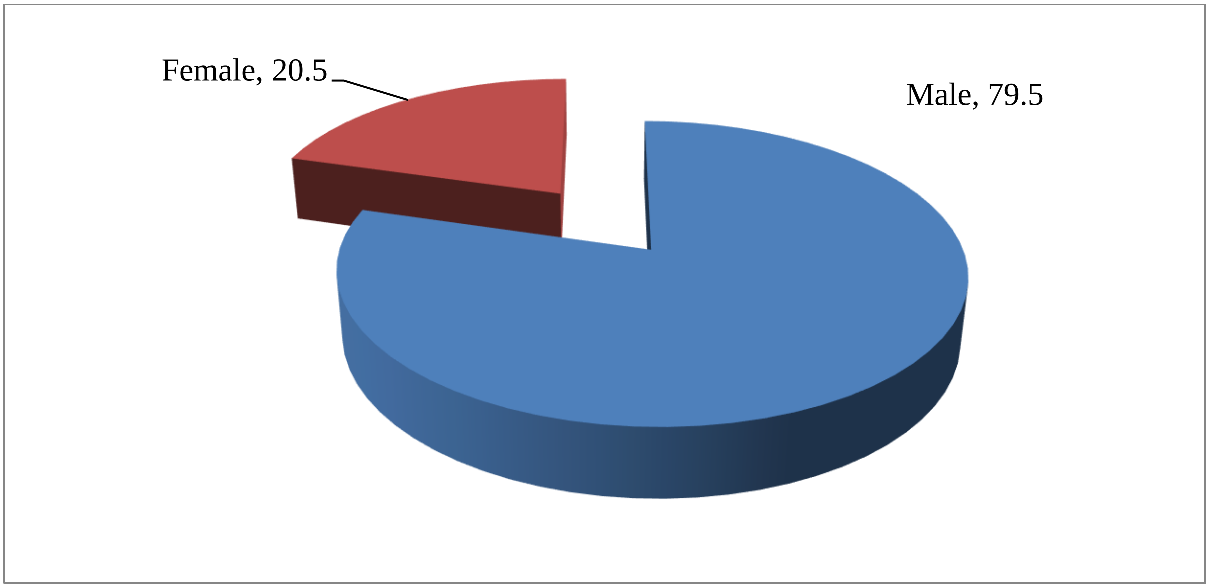


Figure 4. 1.Respondents' Gender

4.3.2Age Bracket

Respondents were also asked to specify their age bracket. Moreover, findings were as depicted in Figure 4.2. 48% of the participants pointed out between 31 and 40 years, 43% pointed out between 41-50 years and finally 9 percent pointed out between 18 and 30 years. Additionally, this denotes that majority of cybercrime departmental heads in Commercial Banks are aged between 31 and 40 years. Moreover, this denotes that participants were able to provide substantial information on cyber resilience techniques.

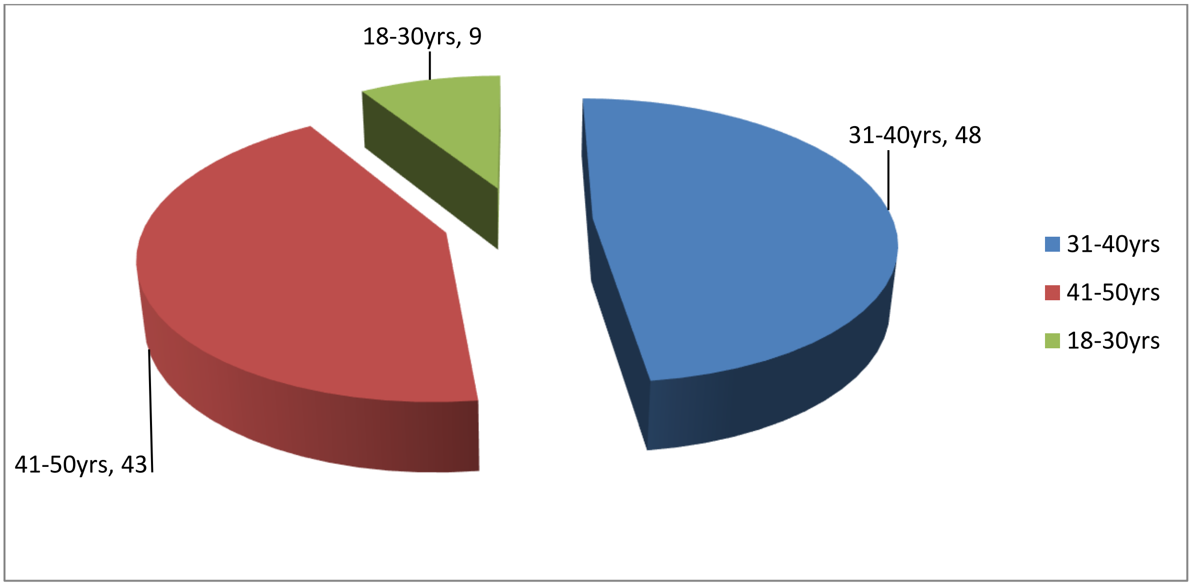


Figure 4. 2.Age Bracket

4.3.3Level of Education

Moreover, participants were requested to indicate their academic level. According to the findings, 73% of the respondents pointed out that they had master's degree and 27% pointed undergraduate degree. This means that majority of the cybercrime departmental heads in Commercial Banks had master's degree as their education level.

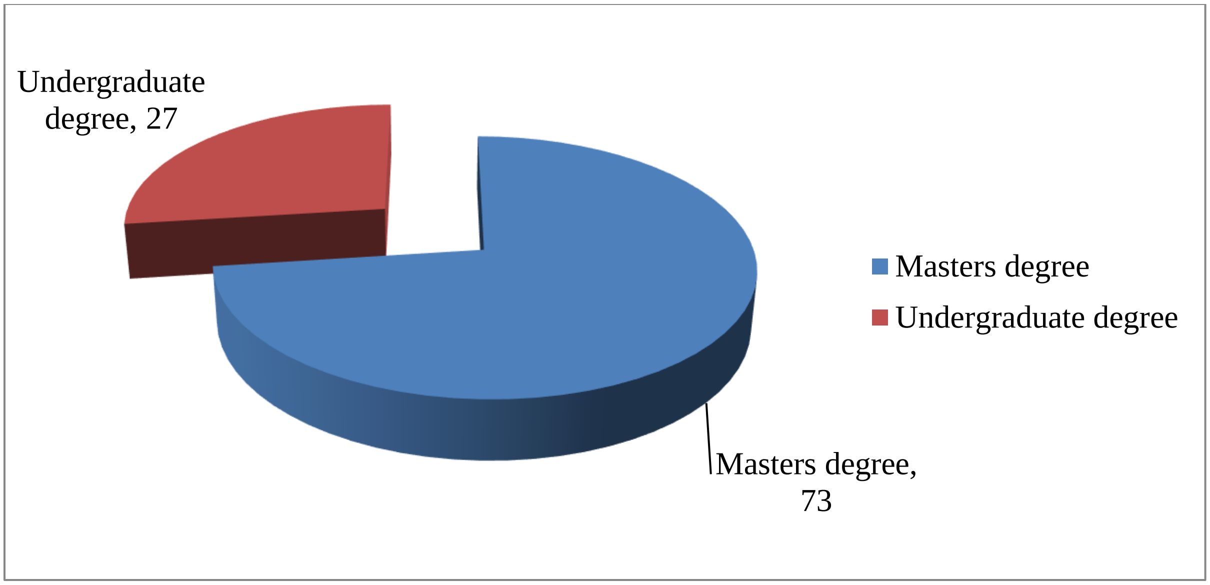
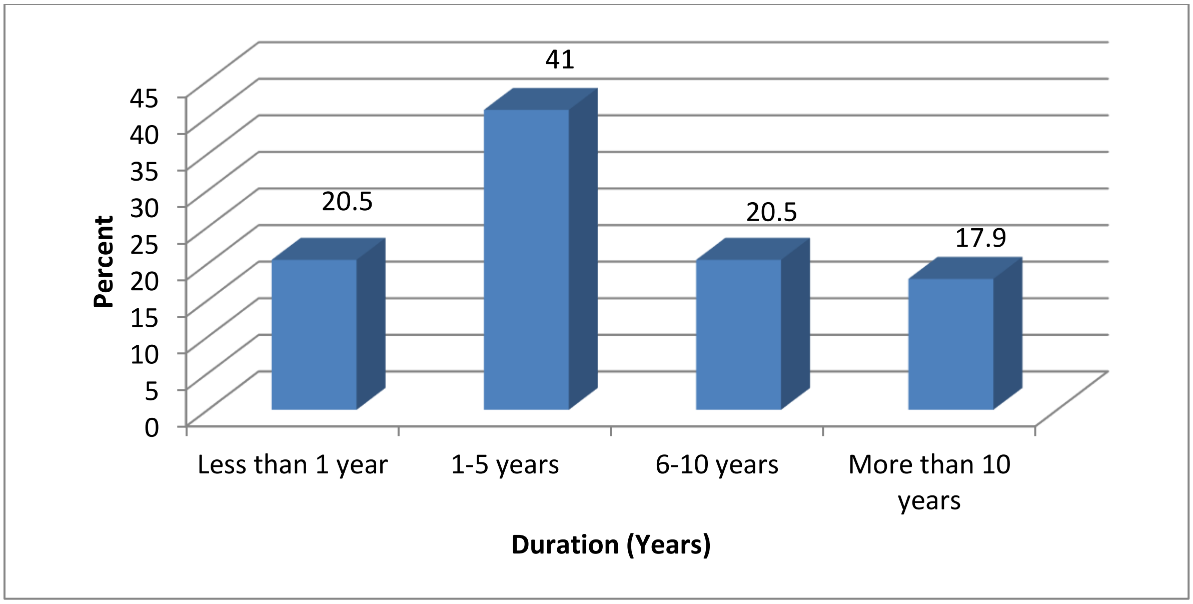


Figure 4. 3. Level of Education

4.3.4 Duration of Time Working in their Organizations

Participants were as well required to show the period they had been in their organizations. According to the study results, 41% of cybercrime departmental heads pointed out that they had been working in their organizations for between 1-5 years, 20.5% pointed out for between 6-10 years, the same percent pointed out for less than 1 year and 17.9% indicated 10 years and above. Moreover, this indicates that large number of cybercrime departmental heads in Kenyan Commercial Banks has not less than five years work experience. This implies that respondents were experienced enough to provide substantial information of cybercrime resilience techniques.

Figure 4. 4. Duration of Working



4.4 Cyber Resilience Techniques Adopted By Commercial Banks

First specific objective was to identify cyber resilience techniques adopted by Kenyan commercial banks.

4.4.1 Cyber Resilience Techniques and Cyber Resilience in Commercial Banks

Respondents were as well asked to specify the extent of adopting cyber resilience methods in the organization. The results obtained were as displayed in Table 4.1. Respondents revealed that their organizations have adopted privilege restriction to a great extent (mean=4.282, std. dv=0.647). Moreover, with (mean=4.000, std. dv=0.649), respondents indicated that organizations had adopted coordinated protection to great extent. Additionally, respondents pointe out by mean of 4.000 (std. dv = 0.649) that their organizations had adopted dynamic positioning to a great extent.

The respondents pointed that their organizations had adopted substantiated integrity to great extent (mean of 3.923, std. dv=0.703). Furthermore, with (mean=3.821, std. dv=0.756), the respondents indicated that their organizations had adopted analytical monitoring to great extent. Additionally, they specified with (mean=3.692, std. dv 0.800) that their organizations had adopted dynamic representation to a great extent. Further, the respondents pointed out that their organizations had adopted deception to moderate extent (mean=3.231, std. dv=1.180).

Table 4. 2. Extent of adopting the cyber resilience techniques

Cyber Resilience Techniques	1	2	3	4	5	Mean	Std.Deviation
Analytical monitoring	0.00	0.00	38.5	41.0	20.5	3.821	0.756
Coordinated protection	0.00	0.00	20.5	59.0	20.5	4.000	0.649
Substantiated integrity	0.00	0.00	28.2	51.3	20.5	3.923	0.703
Deception	0.00	38.5	20.5	20.5	20.5	3.231	1.180
Adaptive response	0.00	0.00	51.3	28.2	20.5	3.692	0.800
Dynamic representation	0.00	0.00	51.3	28.2	20.5	3.692	0.800
Dynamic positioning	0.00	0.00	20.5	59.0	20.5	4.000	0.649
Privilege restriction	0.00	0.00	10.3	51.3	38.5	4.282	0.647

4.4.2. Extent of Cybercrimes Prevention

The respondents were requested to specify the degree to which cyber resilience techniques prevent cybercrimes against the bank. Results obtained were depicted in Table4.2. Study findings found that cyber resilience techniques have prevented unauthorized disclosure or passwords to a great extent, (mean=4.205, std. dv=0.615). With mean of 4.180 (std. dv=0.601), respondents pointed out that cyber resilience techniques had prevented card information skimming to great extent. Moreover, they indicated that cyber resilience techniques had prevented electronic money laundering to great extent, (mean, 4.103, std. dv=1.071). Additionally, they revealed that cyber resilience techniques had prevented impersonation to great extent (mean=4.000, std. dv=0.649). Moreover, respondents indicated that cyber resilience techniques had prevented forgery to great extent (mean=4.000, std. dv = 0.795).

With (mean=3.897, std. dv=0.718), respondents revealed that cyber resilience techniques had prevented email and phishing scams to a great extent. Furthermore, they pointed out that cyber resilience techniques had prevented attacks on transaction channels to a great extent, (mean=3.795, std. dv=0.615). By mean of 3.795 (std. dv=0.615), the respondents revealed that cyber resilience techniques had prevented malware to a great extent. By mean of 3.692 (std. dv=0.800), the respondents indicated that cyber resilience techniques had prevented fraud to a great extent. Furthermore, they pointed out that cyber resilience techniques had prevented fraudulent use of electronic data to a great extent. This is shown by mean of 3.615 (std. dv=0.673). With mean of 3.487 (std. dv=0.683), the respondents indicated that cyber resilience techniques had prevented online intrusion to a moderate extent. Moreover, they revealed that cyber resilience techniques had prevented identity theft to a moderate extent (mean = 3.308, std. dv=0.468).

Table 4. 3. Extent of Cybercrimes Prevention

Cybercrimes	1	2	3	4	5	Mean	Std. Deviation
Email and phishing scams	0.00	0.00	30.8	48.7	20.5	3.897	0.718
Identity theft	0.00	0.00	69.2	30.8	0.00	3.308	0.468
Attacks on transaction channels	0.00	0.00	30.8	59.0	10.3	3.795	0.615
Impersonation	0.00	0.00	20.5	59.0	20.5	4.000	0.649
Fraud	0.00	0.00	51.3	28.2	20.5	3.692	0.800
Forgery	0.00	0.00	30.8	38.5	30.8	4.000	0.795
Unauthorized disclosure or passwords	0.00	0.00	10.3	59.0	30.8	4.205	0.615
Fraudulent use of electronic data	0.00	0.00	48.7	41.0	10.3	3.615	0.673
Online intrusion	0.00	10.3	30.8	59.0	0.00	3.487	0.683
Malware	0.00	10.3	0.00	89.7	0.00	3.795	0.615
Card information skimming	0.00	0.00	10.3	61.5	28.2	4.180	0.601
Electronic money laundering	0.00	10.3	20.5	17.9	51.3	4.103	1.071

4.5 Cyber Resilience Techniques and Cyber Resilience in Commercial Banks

Second objective was to assess association between techniques adopted and the level of cyber resiliency in Kenyan commercial banks.

4.5.1 Adaptive Response

Respondents were asked to indicate the degree to which they agree with various statements pertaining to adaptive response as a cyber-resilience technique in their organization. Results were depicted in Table 4.3. According to the results, the respondents selected in this study agreed with mean of 3.897 (std. dv=0.852) that their organizations take pre-emptive action where appropriate. Moreover, they agreed that their organizations limit consequences of cyber-attacks. This is indicate by mean of 3.667 (std. dv=0.898). Additionally, with mean of 3.487 (std. dv=0.683), they agreed that their organizations use agile as well as alternative operational contingencies to retain minimum operational capacities even during attacks.

These findings conform to Kott, Ludwig & Lange (2017) findings that cyber courses of action (CCoA) are used to respond to particular circumstances by employing agile alternative effective contingencies to retain lowest operational capacity, reduce limit consequences, as well as evade destabilization.

Table 4. 4: Adaptive Response

Adaptive Response	**1**	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**
The organization uses agile and alternative operational contingencies to maintain minimum operational capabilities even during attacks	0.00	10.3	30.8	59.0	0.00	3.487	0.683
Our organization limits consequences of cyber attacks	0.00	10.3	30.8	41.0	17.9	3.667	0.898
Our organization takes pre-emptive action where appropriate	0.00	10.3	10.3	59.0	20.5	3.897	0.852

4.5.2 Analytic Monitoring

The participants in this study were required to point out the extent to which they agree with statements relating to analytic monitoring as a cyber-resilience technique in their organization. Results were depicted in Table 4.4. With mean of 4.180 (std. dv=0.601), respondents agreed that their organizations utilize, gather and analyze data to identify vulnerabilities. These findings conform to Connelly, Allen and Linkov (2017) discoveries that analytic monitoring techniques maximize ability to discover adverse conditions, the extent of that particular adverse condition, stresses and potential or actual damage. However, with (mean=3.308, std. dv=0.655), they were neutral that organizations utilize malware and forensic analysis to assess the actual damage by cyber-attacks.

Table 4. 5: Analytic Monitoring

Analytic Monitoring	**1**	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**
Our organization uses, gathers and analyses data to identify vulnerabilities	0.00	0.00	10.3	61.5	28.2	4.180	0.601
Our organization utilizes malware and forensic analysis to assess the actual damage by cyber-attacks	0.00	10.3	48.7	41.0	0.00	3.308	0.655

4.5.3 Coordinated Protection

Participants were further asked to show their agreement with diverse statements regarding coordinated protection as a cyber-resilience technique in their organization. Results were depicted in Table 4.5. With mean of 4.205 (std. dv=0.615), respondents agreed that the use of coordinated protection makes it much difficult to successfully make an attack. Moreover, they agreed that the use of coordinated protection raises the likelihood of adversary detection (mean=4.000, std. dv=0.649). Respondents further agreed that their organizations use multiple and distinct mechanisms to protect systems and sub-systems as shown by mean of 3.974 (std. dv=0.628). These findings conform to Jegede and Olowookere (2016) arguments that the use of diverse cyber resilience techniques ensures maximum protection of their organizations system and sub-systems.

Table 4. 6: Coordinated Protection

Coordinated Protection	1	2	3	4	5	Mean	Std. Deviation
The organization uses multiple and distinct mechanisms to protect systems and sub-systems	0.00	0.00	20.5	61.5	17.9	3.974	0.628
Use of coordinated protection makes it difficult for an adversary to successfully attack	0.00	0.00	10.3	59.0	30.8	4.205	0.615
Use of coordinated protection raises the likelihood of adversary detection	0.00	0.00	20.5	59.0	20.5	4.000	0.649

4.5.4 Deception

With (mean=3.667, std. dv=1.199), respondents agreed that deception technology causes adversary to misdirect or waste its resources. Nonetheless, they were neutral that deception technology is used to delay the effect of attack. This is indicated by mean of 3.256 (std. dv=1.186). Moreover, respondents were neutral with mean of 3.026 (std. dv=0.903) that their organizations use deception technology to confuse and mislead adversaries.

Table 4. 7: Deception

Deception	1	2	3	4	5	Mean	Std. Deviation
The organization uses deception technology to confuse and mislead adversaries	0.00	38.5	20.5	41.0	0.00	3.026	0.903
Deception technology is used to delay the effect of attack	0.00	41.0	10.3	30.8	17.9	3.256	1.186
Deception technology causes the adversary to misdirect or waste its resources	0.00	30.8	0.00	41.0	28.2	3.667	1.199

4.5.5 Dynamic Representation

The respondents were further asked to point out their agreement level with various statements regarding dynamic representation as a cyber-resilience technique in their organization. Results obtained were depicted in Table 4.7. The respondents were neutral that their organizations make use of dynamic threat modelling as indicated (mean=3.103, std. dv=0.718). Participants were neutral with mean of 3.026 (std. dv = 1.112) that their organizations use dynamic mapping and profiling. Furthermore, the respondents were neutral that their organizations keep on changing systems. This is shown by mean of 2.821 (std. dv=0.756). According to Woodard (2019) deception technology contributes to addressing the key specific problems by allowing an organization to identify complex threats far more rapidly than previously possible, while also lowering the costs associated with identifying more mundane (less technically sophisticated) attacks..

Dynamic Representation	**1**	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**
The organization uses dynamic mapping and profiling	10.3	28.2	10.3	51.3	0.00	3.026	1.112
Our organization makes use of dynamic threat modelling	0.00	20.5	48.7	30.8	0.00	3.103	0.718
Our organization keeps on changing systems	0.00	38.5	41.0	20.5	0.00	2.821	0.756

4.5.6 Dynamic Positioning

The participants were requested to point out their agreement level with various statements regarding dynamic positioning as a cyber-resilience technique in their organization. Results were shown in Table 4.7. The respondents were moderate with (mean=3.205, std. dv=0.767) that organizations ensure asset mobility to change attack surface. Moreover, they were as well neutral that their organizations frequently relocate functionality as shown by mean of 2.923 (std. dv=0.839). Ganin, Kitsak and Linkov (2017) discovered that dynamic positioning methods distribute and also dynamically relocate assets and functionality, resulting in a shift in the attack surface.

Table 4. 8: Dynamic Positioning

Dynamic Positioning	1	2	3	4	5	Mean	Std. Deviation
Our organization frequently relocates functionality	0.00	38.5	30.8	30.8	0.00	2.923	0.839
Our organization ensures asset mobility to change attack surface	0.00	20.5	38.5	41.0	0.00	3.205	0.767

4.5.7 Privilege Restriction

The participants in this study were requested point out the extent to which they agree with statements relating to privilege restriction as a cyber-resilience technique in their organization. Results were as shown in Table 4.8. The respondents further agreed with mean of 4.180 (std. dv=0.601) that use of cyber resilience curtails adversary's ability to take advantage of credentials. These discoveries conform to Fraenkel, 2014) arguments that privilege restriction enables an organization to limit ability to access people's credentials. Moreover, they agreed that their organizations limit the probability of unintended actions by authorized individuals, (mean=3.795, std. dv=0.615). Additionally, they agreed that their organizations restrict the use of systems and sub-systems (mean = 3.590, std. dv = 0.677).

Table 4. 9: Privilege Restriction

Privilege Restriction	1	2	3	4	5	Mean	Std. Deviation
The organization restricts the use of systems and sub-systems	0.00	10.3	20.5	69.2	0.00	3.590	0.677
Our organization limits the probability of unintended actions by authorized individuals	0.00	10.3	0.00	89.7	0.00	3.795	0.615
Use of cyber resilience curtails the adversary's ability to take advantage of credentials	0.00	0.00	10.3	61.5	28.2	4.180	0.601

4.5.8 Substantiated Integrity

The respondents in this study were as well requested to show their agreement with statements regarding substantiated integrity as a cyber-resilience technique in their organization. With (mean=3.410, std. dv = 0.498) the respondents were neutral that their organizations have measures in place to determine whether information streams have been tainted. Moreover, they were neutral that their organizations provide mechanisms to determine whether information stores have been corrupted as indicated by mean of 3.308 (std. dv=0.655). Furthermore, respondents were neutral that their organizations provide mechanisms to ascertain whether essential services have been corrupted. This is indicated by mean of 3.205 (std. dv=0.615). According to Chewning, Lai and Doerfel (2013) substantiated integrity limits the impact as well as possibility that unintentional actions by particular authorized people will jeopardize information.

Table 4. 10: Substantiated Integrity

Substantiated Integrity	**1**	**2**	**3**	**4**	**5**	**Mean**	**Std. Deviation**
The organization provides mechanisms to ascertain whether critical services have been corrupted	0.00	10.3	59.0	30.8	0.00	3.205	0.615
Our organization provides mechanisms to ascertain whether information stores have been corrupted	0.00	10.3	48.7	41.0	0.00	3.308	0.655
Our organization provides mechanisms to ascertain whether information streams have been corrupted	0.00	0.00	59.0	41.0	0.00	3.410	0.498

4.6 Cyber resilience in Commercial Banks in Kenya

Dependent variable in this study was level of cyber resiliency in commercial banks in Kenya and was measured in terms of anticipate, withstand, recover and evolve.

4.6.1 Extent of Achieving Cyber Resilience Goals

Respondents were requested to specify the degree to which their organizations had achieved cyber resilience goals during cyber-crime. The results obtained were as depicted in Table 4.4. From the study findings, the respondents pointed out that their organizations had achieved change during cyber-crime to a great extent. This is shown by mean of 4.077 (std. dv=0.532). Moreover, with mean of 3.897 (std. dv=0.307), respondents indicated that their organizations had achieved recovery during cyber-crime to a great extent. Furthermore, they pointed out that their organizations had achieved withstanding during cyber-crime to a great extent. This is mean of 3.692 (std. dv=0.655). Moreover, with mean of 3.513 (std. dv=0.721), respondents revealed that their organizations had achieved anticipation during cyber-crime to a great extent. This implies that their organizations had achieved cyber resilience goals to a great extent.

Table 4. 11. Extent of Achieving Cyber Resilience Goals

Cyber Resilience Goals	1	2	3	4	5	Mean	Std.Deviation
Anticipate	0.00	10.3	30.8	56.4	2.6	3.513	0.721
Withstand	0.00	10.3	10.3	79.5	0.00	3.692	0.655
Recover	0.00	0.00	10.3	89.7	0.00	3.897	0.307
Evolve	0.00	0.00	10.3	71.8	17.9	4.077	0.532

4.6.2 Frequency of Service Disruptions

The respondents were requested to indicate how frequent their organizations experience service disruptions. The findings were shown in Figure 4.5. According to the findings, 82.1% of the participants indicated that their organizations experience service disruptions every month and 17.9% indicated every six months. This implies that majority of Kenyan commercial banks experience service disruptions every month.

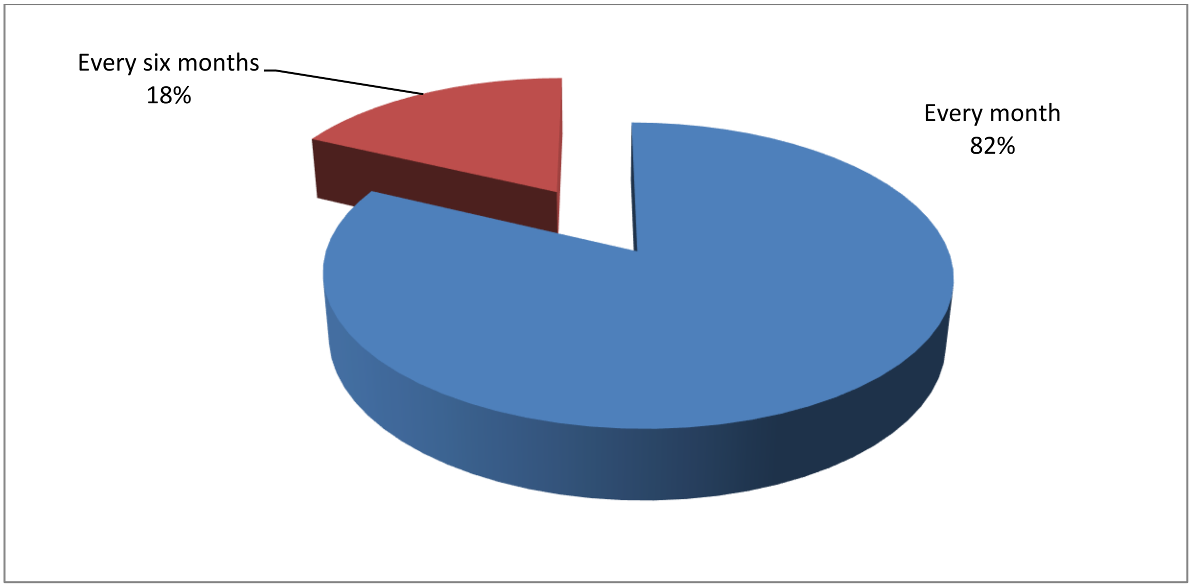


Figure 4. 5. Frequency of Service Disruptions

4.6.3 Duration of Recovery from Incidences

The participants were also asked to specify the period taken to recover from incidences. From the study, 54.1% of the respondents indicated that it takes between 1 and 2 days to recover from the incidences, 40.5% indicated more than 5 days and 5.4% between 3 and 4 days. This implies that majority of the Kenyan commercial banks take between 1 and 2 days to recover from cyber-crime incidences.

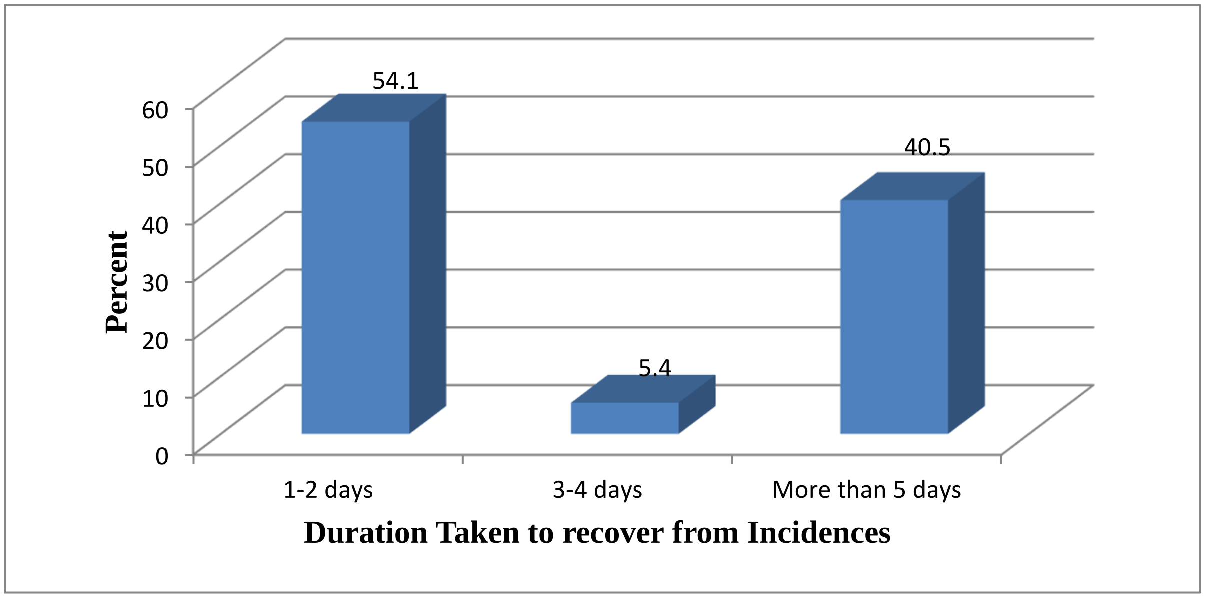


Figure 4. 6. Duration Taken to Recover from Incidences

4.6.4 Number of Incidences Prevented

Participants were as well invited to indicate total number of incidences that are prevented within a month in their organizations. From the results, 54.1% of the participants indicated that less than 5 incidences are prevented within a month in their organizations, 35.1% pointed out between 6 and 10incidences, 10.8% indicated more than 10 incidences, the same per cent pointed out 3 incidences, 8.1% indicated 7 incidences and the same per cent indicated 2 incidences. This implies that less than 5 incidences are prevented within a month in commercial bank.

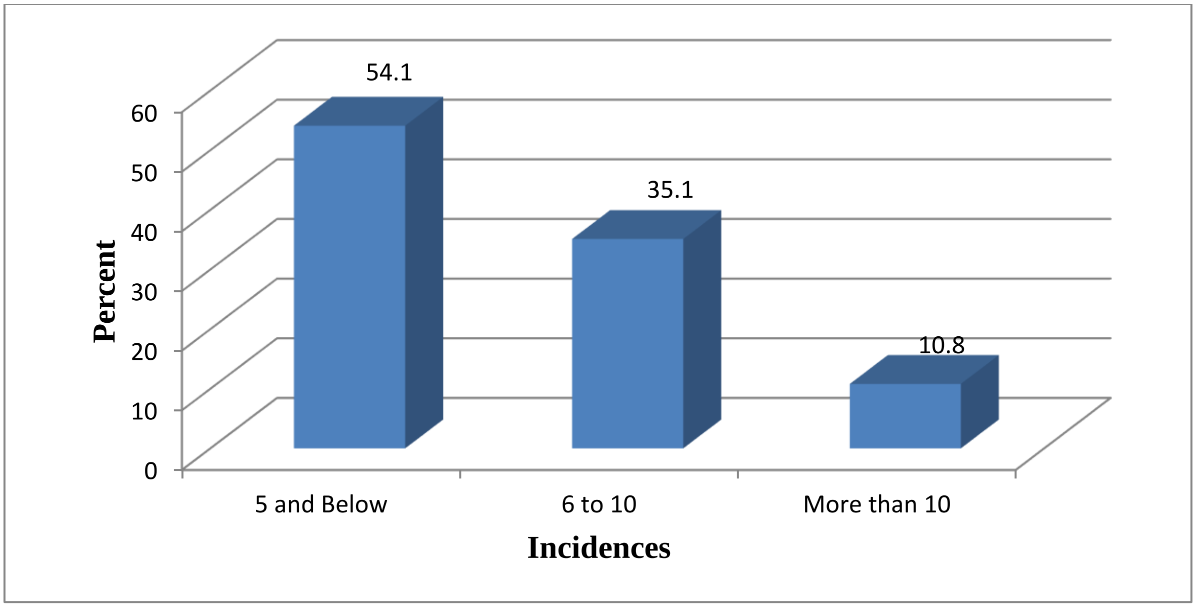


Figure4. 7. Number of Incidences

4.7 Recommended Methods to Improve Cyber Resiliency

The third objective was to recommend the appropriate methods to improve cyber resiliency for commercial banks. The respondents were requested to point out ways in which cyber resiliency in Kenya commercial banks can be improved. The respondents indicated that the cyber resiliency in Kenya commercial banks can be improved through training, outsourcing of cyber security control measures and conducting staff awareness campaigns. Moreover, the respondents indicated that cyber resiliency can be improved by ensuring risk response planning process is executed during as well as after the incident, ensuring their organizations implement improvements by integrating lessons learned from previous and current detection/response activities, as well as ensuring their organizations successfully implement recovery planning procedures as well as processes to restore assets and/or systems adversely effected by cyber-security incidents, ensuring tests are carried out to ensure response as well as recovery activities, for example forensic analysis, establishing the effect of occurrences, and ensuring which anomalies as well as occurrences are discovered and also their possible effect is well understood.

Furthermore, the respondents revealed that cyber resilience can be improved by implementing security constant monitoring abilities to regulate cyber-security events and validate the effectiveness of protective measures such as network as well as physical activities, maintaining detection processes to provide consciousness of anomalous events, managing protective technology to make sure that system as well as asset security and resilience are related to organizational policies, agreements and procedures, and ensuring protections for identity management, access control within their organizations including physical as well as remote access and by enforcing multi-factor authentication.

In addition, the respondents indicated that cyber resilience can be improved by establishing protection of data security in harmony with organizations' risk strategy to safeguard confidentiality, integrity, as well as access to information, as well as to identify asset vulnerabilities, risks to internal as well as external organizational resources, and risk response activities and risk response as the foundation for the organization's risk assessment.

In addition, respondents revealed that cyber resilience can be improved by identifying risk management strategy including developing risk tolerances, priorities and constraints and also identifying tangible and also software assets to pave the way for asset management program.

4.8 Inferential Statistics

This study employed correlation as well as regression analysis to assess the relationship between cyber resilience techniques and cyber resilience in commercial banks.

4.8.1 Correlation Analysis

This researcher deployed Pearson correlation to assess association between study variables. Results were displayed in Table 4.11. There is a very strong association between adaptive response and cyber resilience (r= 0. 956, p-value=0.000). Significance level (0.05) was greater than p value (0.000) hence indicating a significant association. These results concur with the results of Dupont (2019) that adaptive response has a positive effect on cyber resilience in Nigeria's business environment.

The results found a very strong relationship between analytic monitoring and cyber resilience (r= 0. 916, p-value=0.000). This correlation was deemed significant because the p-value was less than significant level. The results conform to Boyes (2015) discoveries that analytic monitoring influences cyber resilience internet banking in Jordan significantly.

Furthermore, results show a strong association between coordinated protection and cyber resilience (r=0.860, pvalue=0.000). Correlation was deemed significant as p.value was below 0.05. Results conform to Graubart (2013) findings that coordinated protection influences the cyber resilience by raising the likelihood of adversary detection.

The results show that there was a weak relationship between deception and cyber resilience (r=0.298, p-value=0.066). Correlation however was considered insignificant as p.value 0.066 was greater than 0.05 which is significant level. Ondieki (2013) found that deception technology influences cyber resilience by delaying the effect of attack in an organization.

The study found a very strong association between dynamic representation and cyber resilience (r=0.871, p-value=0.000). Moreover, significant level of 0.05 was above p value (0.000) hence indicating a significant association. These results concur with Ganin, Kitsak and Linkov (2017) discoveries that dynamic representation has positive effect on the cyber-crime resilience in Kenyan commercial Banks.

Additionally, a very strong association between dynamic positioning and cyber resilience (r= 0.823, p-value =0.000) was reported by the study. Significant level of 0.05 was above p-value (0.000) hence indicating a significant association. These results concur with Chewning, Lai and Doerfel (2013) discoveries that dynamic positioning increases ability to recover quickly from non-adversarial events.

Moreover, the results established a strong association between privilege restriction and cyber resilience (r=0.722, p-value=0.000). Additionally, significant level was above p-value (0.000) hence indicating a significant association. These results concur with the results of Greene, Galambos and Lee (2014) that privilege restriction influences cyber resilience in NIC Bank of Kenya in a significant way.

The results also show a very strong relationship between substantiated integrity and cyber resilience (r= 0.956, p-value =0.000). Additionally, significant level was above the p value (0.000) hence indicating a significant association. These results concur with the findings of Bodeau, Brtis and Graubart, (2013) that substantiated integrity has a positive effect of cyber resilience on online banking in Commercial Banks in Kenya.

Table 4. 12: Correlations Coefficients

		CS	AR	AM	CP	DE	DR	DP	PR	SI
Cyber Resilience (CS)	Pearson Correlation	1								
	Sig. (2-tailed)									
	N	37								
Adaptive Response (AR)	Pearson Correlation	.956**	1							
	Sig. (2-tailed)	.000								
	N	37	37							
Analytic Monitoring (AM)	Pearson Correlation	.916**	.132	1						
	Sig. (2-tailed)	.000	.108							
	N	37	37	37						
Coordinated Protection (CP)	Pearson Correlation	.860**	.293	.851**	1					
	Sig. (2-tailed)	.000	.071	.000						
	N	37	37	37	37					
Deception (DE)	Pearson Correlation	.298	.420**	.368*	.049	1				
	Sig. (2-tailed)	.066	.008	.021	.769					
	N	37	37	37	37	37				
Dynamic Representation (DR)	Pearson Correlation	.871**	.425**	.256	.321*	.298	1			
	Sig. (2-tailed)	.000	.007	.115	.046	.066				
	N	37	37	37	37	37	37			
Dynamic Positioning (DP)	Pearson Correlation	.823**	.256	.364*	.144	.132	.224	1		
	Sig. (2-tailed)	.000	.115	.023	.380	.108	.170			
	N	37	37	37	37	37	37	37		
Privilege Restriction. (PR)	Pearson Correlation	.722**	.293	.256	.256	.564**	.375*	.144	1	
	Sig. (2-tailed)	.000	.071	.115	.115	.000	.019	.380		
	N	37	37	37	37	37	37	37	37	
Substantiated Integrity (SI)	Pearson Correlation	.903**	.239	.287	.105	.717**	.293	.256	.453**	1
	Sig. (2-tailed)	.000	.144	.076	.526	.000	.071	.115	.004	
	N	37	37	37	37	37	37	37	37	37

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

4.8.2 Regression Analysis

Multivariate regression analysis was employed to determine effect of cyber resilience techniques (adaptive response, dynamic positioning, deception, coordinated protection, dynamic representation, analytic monitoring, substantiated integrity and privilege restriction) on cyber resilience in commercial banks. The r-squared was deployed to show the proportion of dependent study variable that independent variables can accounted for. R-squared was 0.805, which denotes that independent variables (adaptive response, dynamic positioning, deception, coordinated protection, dynamic representation, analytic monitoring, substantiated integrity and privilege restriction) could explain 80.5% of the dependent variable (cyber resilience in commercial banks).

Table 4.13:Model Summary

Model	R	RSquare	AdjustedR Square	Std.Error of Estimate
1	0.897[a]	.805	.792	.04092

a. Predictors: (Constant), Substantiated Integrity, Coordinated Protection, Deception, Dynamic Representation, Analytic Monitoring, Dynamic Positioning

This research used analysis of variance in assessing whether model employed was good fit for the data. Additionally, F-calculated (518.120) was higher than F.critical value (2.266) and p value (0.000) was less than the significant level (0.05). Therefore, the model was a good fit for the data and could be employed in explaining the influence of cyber resilience techniques (adaptive response, dynamic positioning, deception, coordinated protection, dynamic representation, analytic monitoring, substantiated integrity and privilege restriction) on cyber resilience in commercial banks.

Table 4.14: Analysis of Variance

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.930	8	0.991	518.120	.000[b]
	Residual	.054	28	0.002		
	Total	8	36			

a. DependentVariable: Cyber Resilience
b. Predictors:(Constant), Substantiated Integrity, Coordinated Protection, Deception, Dynamic Representation, Analytic Monitoring, Dynamic Positioning

Regression model was as shown below:

$$Y = 2.162 +0.194X_1 + 0.852X_2 +0.376X_3 +0.148X_4 +0.410X_5 + 0.229X_6 +0.201X_7 +0.519X_8$$

The results showed that adaptive response has significant positive effect on cyber resilience in Kenyan commercial banks (β_1=0.194, p value=0.033). This denotes that enhancement in adaptive response would result in 0.194 improvements in cyber resilience of commercial banks. Moreover, the relationship was deemed as significant as p-value (0.033) was below significance level. The findings conform to Dupont (2019) discovery that adaptive response has a positive effect on cyber resilience in Nigeria’s business environment.

Results also discovered that analytic monitoring has significant positive impact on cyber resilience of Kenyan commercial banks (β_2=0.852, p value= 0.000). Moreover, this denotes that improvement in analytic monitoring would result to 0.852 improvements in cyber resilience of commercial banks. The association of this variable was regarded significant due to the fact that p-value=0.000 was not more than 0.05. Results conform to Boyes (2015) findings that analytic monitoring influences cyber resilience Internet banking in Jordan significantly.

Further, results discovered that coordinated protection has significant positive effect on cyber resilience of commercial banks (β_3=0.376, p.value=0.002). This implies that enhancement in coordination protection would result to 0.376 improvements in cyber resilience of commercial banks. The association was regarded significant since p.value (0.002) was below 0.05. The findings conform to Graubart (2013) discoveries that coordinated protection influences the cyber resilience by raising the likelihood of adversary detection.

Furthermore, results show that deception has insignificant impact on cyber resilience of Kenyan commercial banks (β_4=0. 148, p value=0.134). The association was regarded as insignificant as p-value (0.134) was below significance level (0.05). Findings are contrary to the findings of Ondieki (2013) that deception technology influences cyber resilience by delaying the effect of attack in an organization.

The results showed that dynamic representation has significant effect on cyber resilience (β_5=0.410, p value=0.000) which implies that enhancement in dynamic representation result in 0.410 improvement in cyber resilience of commercial banks. Moreover, association was regarded significant because p.value was below significance level. Moreover, findings conform to Ganin, Kitsak and Linkov (2017) discoveries that dynamic representation has a positive influence on the cyber-crime resilience in Kenyan commercial Banks.

The results also show that dynamic positioning has significant positive impact on cyber resilience of commercial banks (β_6=0.229, p.value=0.081). This means that enhancement in dynamic positioning would result in 0.229 improvements in cyber resilience of commercial banks. Moreover, the relationship was regarded significant since p-value of 0.000 was below significance level. The findings conform to Chewning, Lai and Doerfel (2013) that dynamic positioning increases ability to recover from diverse non-adversarial events

Further, results discovered that privilege restriction has significant positive effect on cyber resilience of commercial banks (β_7=0.201, p.value=0.021). This means that enhancement in privilege restriction would result in 0.201 improvements in cyber resilience of commercial banks. Moreover, the relationship was regarded significant because p-value of 0.021 was below significant level. The findings conform to the discoveries of Greene, Galambos and Lee, (2014) that privilege restriction influences cyber resilience in NIC Bank of Kenya in a significant way.

Furthermore, results show that substantiated integrity has significant positive effect on cyber resilience of commercial banks (β_8=0.519, p-value= 0.000). Moreover, this implies that improvement in substantiated integrity would result in 0.519 improvements in cyber resilience of commercial banks. Moreover, the relationship was significant given that p-value 0.134 was below significance level. The findings conform to Bodeau, Brtis and Graubart, (2013) findings that substantiated integrity has a positive effect of cyber resilience on online banking in Commercial Banks.

Table 4. 15: Regression Coefficients

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	2.162	0.221		9.783	0.000
	Adaptive Response	0.194	0.073	0.201	2.658	0.033
	Analytic Monitoring	0.852	0.165	1.008	5.164	0.000
	Coordinated Protection	0.376	0.107	0.383	3.514	0.002
	Deception	0.148	0.152	0.184	0.974	0.134
	Dynamic Representation	0.410	0.095	0.424	4.316	0.000
	Dynamic Positioning	0.229	0.081	0.248	2.841	0.014
	Privilege Restriction	0.201	0.072	0.221	2.792	0.021
	Substantiated Integrity	0.519	0.104	0.608	4.990	0.000

a. Dependent Variable: Cyber Resilience

CHAPTER FIVE
SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter entails summary of study results, conclusions reached at, recommendation made as well as suggestions for more studies as per study objectives. The researcher sought to investigate influence of cyber resilience techniques on cyber resilience in Kenyan commercial banks. The study objectives were meant to identify techniques adopted by commercial banks; the association between techniques adopted and also the level of cyber resiliency in Kenyan commercial banks; and recommend methods to improve cyber resiliency for commercial banks.

5.2 Summary of Findings

This sub-section covers summary of findings pertaining to impact of cyber resilience techniques adopted by Kenyan commercial banks and relationship between techniques adopted and level of cyber resiliency.

5.2.1 Cyber Resilience Techniques Adopted By Commercial Banks

The first specific objective was to identify cyber resilience techniques adopted by Kenyan commercial banks. Moreover, the researcher found that commercial banks have adopted privilege restriction, coordinated protection, dynamic positioning, substantiated integrity, analytical monitoring and dynamic representation to a great extent. However, deception as a cyber resilience technique had been adopted to a moderate extent.

The study found that cyber resilience techniques prevented cybercrimes against the bank. Specifically, the study found that cyber resilience techniques had prevented unauthorized disclosure or passwords against banks to a great extent. In addition, cyber resilience techniques had prevented card information skimming and electronic money laundering to great extent. Further, cyber resilience techniques had prevented impersonation, forgery and email and phishing scams against banks to great extent. Moreover, the study found that cyber resilience techniques had prevented attacks on transaction channels, malware and fraud against banks to great extent. Additionally, cyber resilience techniques had prevented fraudulent use of electronic data, online intrusion and identity theft against to a moderate extent.

5.2.2 Relationship between Techniques Adopted and the Level of Cyber Resiliency

The second objective was to examine the association between techniques adopted and the level of cyber resiliency in Kenyan commercial banks. The study discovered that adaptive response has significant positive impact on cyber resilience in commercial banks. The study discovered that commercial banks take pre-emptive action where appropriate. Moreover, the study revealed that agreed that the organization limits consequences of cyber-attacks. In addition, the research found that commercial banks use agile as well as alternative effective contingencies in order to maintain lowest operational capabilities even during attacks.

The study discovered that analytic monitoring influences cyber resilience of commercial banks significantly and positively. Additionally, the study established that commercial banks in Kenya utilize, gather and analyse data to identify vulnerabilities. However, commercial banks in Kenya moderately utilize malware and forensic analysis to assess the actual damage by cyber-attacks.

Further, coordinated protection has significant positive impact on cyber resilience of commercial banks. Additionally, the study established that use of coordinated protection makes it much difficult for an adversary to successfully attack. In addition, the use of coordinated protection raises the likelihood of adversary detection. Further, commercial banks in Kenya utilize multiple and distinct mechanisms to protect systems and sub-systems.

Furthermore, the study found that deception has an insignificant influence on cyber resilience of commercial banks. Moreover, deception technology causes adversary to misdirect or waste its resources. Nonetheless, deception technology is moderately used to delay the effect of attack. Moreover, commercial banks in Kenya moderately use deception technology to confuse and mislead adversaries.

The findings indicated that dynamic representation has significant effect on cyber resilience in commercial banks. The research found that commercial banks moderately utilize dynamic threat modelling. Furthermore, commercial banks moderately use dynamic mapping and profiling. The study also found that commercial banks in Kenya moderately keep on changing systems. Generally, dynamic representation addresses the key pain points by enabling an organization to identify complex threats much more rapidly than before, while also lowering the costs associated with sensing more mundane (technically less sophisticated) attacks..

The study found that dynamic positioning has significant positive impact on cyber resilience of commercial banks. Moreover, the study discovered that commercial banks in Kenya moderately ensure asset mobility to change attack surface. Moreover, the study found that commercial banks at times relocate functionality. Dynamic positioning methods dynamically distribute and also relocate organizations' assets as well as functionality, thereby altering attack surface.

The study also found that that privilege restriction has significant positive impact on cyber resilience. The findings revealed that use of cyber resilience curtails adversary's ability to fully exploit credentials. Privilege restriction enables an organization to limit ability to take access people's credentials. In addition, commercial banks in Kenya limit the probability that unintended actions by authorized individuals. In addition, commercial banks restrict the use of systems and sub-systems.

Furthermore, substantiated integrity has significant positive impact on cyber resilience of Kenyan commercial banks. Moreover, commercial banks in Kenya moderately provide mechanisms for determining whether information streams have been tampered with. In addition, commercial banks in Kenya moderately provide mechanisms for determining whether information stores have been corrupted. Furthermore, the study discovered that commercial banks moderately provide mechanisms to ascertain whether critical services have been corrupted.

5.3 Conclusions

The study thus concludes that commercial banks operating in Kenya had adopted privilege restriction, coordinated protection, dynamic positioning, substantiated integrity, analytical monitoring and dynamic representation to a great extent. However, deception as a cyber resilience technique had been adopted to moderate extent. Moreover, the study also concludes that cyber resilience techniques had prevented unauthorized disclosure or passwords, card information skimming, electronic money laundering, impersonation, forgery and email and phishing scams, attacks on transaction channels, malware and fraud against banks to a great extent. However, cyber resilience techniques had prevented fraudulent use of electronic data, online intrusion and identity theft against to moderate extent.

The study concludes that cyber resilience techniques such as adaptive response, coordinated protection, dynamic representation, dynamic positioning, analytic monitoring, privilege restriction and substantiated integrity had significant positive impact on cyber resilience in commercial banks. Additionally, the research concludes that deception has insignificant influence on cyber resilience of Kenyan commercial banks.

5.3 Recommendations

The study found that deception as a cyber-resilience technique was not used in some commercial banks. This study thus recommends that management ought to adopt deception technology to cause adversaries misdirect or waste their resources, delay the effect of attack and confuse and mislead adversaries.

The study found that analytic monitoring plays a major role in prevention of cyber-crime and in the achievement of cyber resilience. The researcher thus recommends that the management need to makes use of analytic monitoring to gather, analyse and utilize data to identify vulnerabilities as well as utilize malware and forensic analysis to assess the actual damage by cyber-attacks.

The study found that coordinated protection influences cyber resiliency in commercial banks. Therefore, commercial banks should makes use of multiple and distinct mechanisms to protect systems and sub-systems so as to raise the likelihood of adversary detection.

The study discovered that dynamic positioning has positive impact on cyber resilience in Kenyan commercial banks. This study therefore recommends that the management of commercial banks ought to adopt dynamic positioning as a cyber-resilience technique so as to frequently relocate functionality and ensure asset mobility to change attack surface in an effort to reduce the threat and impact of cyber-attacks.

The study established that privilege restriction has positive impact on cyber resilience in Kenyan commercial banks. The study recommends therefore that the management should develop internal policies to restrict the use of systems and sub-systems in order to limit the probability that unintended actions by authorized individuals.

The study established that cyber resiliency in Kenya commercial banks can be improved through training. Therefore, the management should ensure regular training to impart the employees with knowledge on different cyber resilience techniques that can help limit the likelihood of any action planned by unauthorized personnel succeeding.

The study revealed that cyber resiliency in Kenya commercial banks can be improved by identifying supply chain risk management strategy. This study therefore recommends that the management should identify risk management method for the organization like establishing risk tolerances, constraints, priorities, risk tolerances, as well as assumptions employed to support risk decisions related with supply chain risks management.

Moreover, the study revealed that cyber resiliency can be improved by identifying physical as well as software assets available within the organization. Therefore the management ought to identify organization assets so that the asset management programs are in line with available assets.

The study further established that cyber resiliency in Kenya commercial banks can be improved by managing protective technology. This study hence recommends that the management should properly manage the protective technology so as to ensure that security as well as resilience of assets and systems are consistent with policies and procedures of the organization.

5.4 Recommendations for Further Studies

The purpose of performing this research was to assess influence of cyber resilience techniques on cyber resilience in Kenyan commercial banks. However, other financial institutions in Kenya including microfinance banks as well as SACCOs also experience cyber-attacks. The study therefore recommends further studies to the extent of adoption of cyber resilience techniques in other financial institutions in Kenya. Additionally, the study discovered that 80.5% of the cyber resilience in commercial banks in Kenya could be explained by cyber resilience techniques. The study recommends that further studies ought to be done to examine other factors affecting cyber resilience in commercial banks.

REFERENCES

AbuShanab, E. & Pearson, J.M. (2007). Internet banking in Jordan: The unified theory of acceptance and use of technology (UTAUT) perspective. Journal of Systems and Information Technology, 9(1), 78-97.

Adams, J. (2014). *Research methods for business and social science students*. New Delhi: SAGE Publications.

Adewoye, J. O. (2013). Impact of Mobile Banking on Service Delivery in the Nigerian Commercial Banks. *International Review of Management and Business Research, 2*(2), 32-45.

Africa Cyber Security Report (2020). *Cyber Security Skills Gap.* Retrieved from https://www.serianu.com

Ahiauzu, L. U. & Jaja, S. A. (2015). Process Innovation and Organizational Resilience in. *International Journal of Managerial Studies and Research, 3*(11), 102-111

Ariful, H., Sachin, S., Kimberly, G. & Bheshaj, K. (2016). Realizing Cyber-Physical Systems Resilience Frameworks and Security Practices. *Security in Cyber-Physical Systems, 23,* 1-37.

Atwell, R.C., Schulte, L.A. & Westphal, L.M. (2019). *Linking Resilience Theory and Diffusion of Innovations Theory to Understand the Potential for Perennials in the U.S. Corn Belt.* Retrieved from https://lib.dr.iastate.edu

Babbie, E.R. (2017). *The Basics of Social Research*. Boston: Cengage Learning.

Barkan, S. (2016). *Criminology: A sociological understanding* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. New York: Free Press.

Bicknell, P., Heinbockel, K., Laderman, E. & Serrao, G. (2017). *Cyber Resiliency against Supply Chain Attacks.* Retrieved from https://csrc.nist.gov/

Bodeau, D. & Graubart, R. (2017). *Cyber Resiliency Design Principles*. Retrieved from https://www.mitre.org

Bodeau, D., Brtis, J. & Graubart, R. (2013). *Resiliency Techniques for Systems of-Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain.* Retrieved from https://www.mitre.org

Borum, R., Felker, J. & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security, 23*(3), 317-332.

Boyes, Hugh. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review, 5*, 28-34.

Bryman, A. & Cramer, D. (2012). *Quantitative Data Analysis with SPSS Release 8 for Windows.* New York: Routledge

Central Bank of Kenya (2019). *Guidelines on Cybersecurity: For Payment Service Providers*. Retrieved from https://www.centralbank.go.ke/

Chesaina, F., & Gitonga, E. (2019). Service Delivery and Performance of Kenya Commercial Bank Limited: A Critical Review of Literature. *International Journal of Current Aspects*, *3*(2), 71-82.

Chewning, L. V., Lai, C.H. & Doerfel, M.L. (2013). Organizational Resilience and Using Information and Communication Technologies to Rebuild Communication Structures. *Management Communication Quarterly*, 27(2), 237-263.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608.

Colicchia, C., Creazza, A. & Menachof, D.A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management, 24*(2), 215-240.

Collier, Z. A., Walters, S. & DiMase, D. (2014). A semi-quantitative risk assessment standard for counterfeit electronics detection. *SAE International Journal of Aerospace, 7*(1), 171–181

Communication Authority of Kenya (2020). *National Cyber Security Report for the Period January - March 2020*. Retrieved from https://ca.go.ke/

Connelly, E. B., Allen, C. R. & Linkov, I. (2017). Features of resilience. *Environment Systems and Decisions, 37*(1), 46–50.

Cope, S. (2012). Assessing rational-choice models of budgeting--from budget-maximizing to bureaushaping: a case study of british local government. *Journal of Public Budgeting, Accounting & Financial Management, 12*(4), 598-624.

Creado, Y. & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime, 27*(3), 771-780.

Creswell, J.W. (2014). *Research design. Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks CA: Sage.

DiMase, D., Collier, Z. & Heffner, K. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions, 35*, 10-17.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity, 5*(1), 1-13.

Egbert, J. (2015). *Writing education research: Guidelines for publishable scholarship*. Hoboken: Taylor and Francis.

Farayibi, A. (2016). *Service Delivery and Customer Satisfaction in Nigerian Banks.* Retrieved from https://ssrn.com/abstract=2836963

Fraenkel, J. R. (2014). *How to design and evaluate research in education*. New York: McGraw-Hill Education.

Ganin, A., Kitsak, M. & Linkov, I. (2017). Resilience and efficiency in transportation networks. *Science Advances, 3*(12), e1701079

Ghadge, A., Caldwell, N. D. & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management, 25*(2), 223-240.

Greene, R. Galambos, C. & Lee, Y. (2014). Resilience Theory. *Journal of Human Behavior in the Social Environment, 8*(4), 75-91.

Greenfield, T. & Greener, S. (2016). *Research Methods for Postgraduates*. London: John Wiley Sons Limited.

Gupta, A. & Nisar, T. (2016). Service quality and delivery in banking services—An Indian perspective. *Cogent Business & Management, 3*(1), 43-65.

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things, 11,* 100204.

Hirsch, P.B. (2021). Building a new resilience. *Journal of Business Strategy, 42*(2), 143-146.

Hollnagel, E., Woods, D. D., & Leveson, N. C. (2006). *Resilience engineering: Concepts and precepts.* Aldershot: Ashgate.

Jegede, A. E. & Olowookere, I. E. (2016). Cyber Risks and Fraud in the Nigeria's Business Environment: A Postmortem of Youth Crime. *Journal of Social and Development Sciences, 5*(4), 258-265.

Kosutic, D. & Pigni, F. (2020). Cyber-security: investing for competitive outcomes. *Journal of Business Strategy, 32,* 54-78.

Kott, A., & Abdelzaher, T. (2014). Resiliency and robustness of complex systems and networks. *Adaptive Dynamic and Resilient Systems, 67,* 67–86

Kott, A., Ludwig, J., & Lange, M. (2017). Assessing mission impact of cyberattacks: Toward a model-driven paradigm. *IEEE Security and Privacy, 15*(5), 65–74.

Leonard, C., Ogara, S. & Liyala, S. (2020). An Understanding Of The Cyber Security Threats And Vulnerabilities Landscape: A Case Of Banks In Kenya. *Journal of Information Technology, 7,* 258-263.

Linkov, I. (2018). Fundamental Concepts of Cyber Resilience. Retrieved from https://arxiv.org/ftp/arxiv/papers/1806/1806.02852.pdf

Manyange, N. M. & Atuhairwe, A. (2016). Effects of E-Banking on Service Delivery in Commercial Banks in Western Uganda- A Case of Centenary Bank Ishaka Branch. *Scholars Journal of Economics, Business and Management*, *3*(4), 157-160.

Manyange, N. M., Adeline, A. & Nyabuga, D.O. (2016). Effects of E-Banking on Service Delivery in Commercial Banks in Western Uganda- A Case of Centenary Bank Ishaka Branch. *Scholars Journal of Economics, Business and Management, 3*(4), 157-160.

Mayunga, M.O. (2019). *Developing and Assessing a Cyber-Resilience Framework for Kenyan Banks.* Retrieved from http://repository.anu.ac.ke

Mileski, J. Clott, C. & Galvao, C.B. (2018). Cyberattacks on ships: a wicked problem approach. *Maritime Business Review, 3*(4), 414-430.

Ngugi, B. (2019). *Police probe 130 bank cyber fraud suspects*. Retrieved from https://www.businessdailyafrica.com

Njoroge, E. W. (2020). Effect of Cyber Crime Related Costs on Development of Financial Innovation Products and Services: A Case Study of Nic Bank of Kenya. *Journal of Information Technology, 7*, 258-263.

Nyawanga, J. O. (2015). *Meeting the Challenge of Cyber Threats in Emerging Electronic Transaction Technologies in Kenyan Banking Sector*. Retrieved from http://erepository.uonbi.ac.ke

Nyiranzabamwita, R. & Harelimana, J.B. (2019). The Effect of Electronic Banking on Customer Services Delivery in Commercial Banks in Rwanda. *Enterprise Risk Management, 5*(33), 10-25.

Odhiambo, M. O. (2018). *Effect of Cyber Securities Strategies on Implementation of Online Banking: A Survey of Commercial Banks in Kenya*. Retrieved from http://ir.jkuat.ac.ke

Odonkor, A.A. (2020). *Unveiling the cost of cybercrime in Africa*. Retrieved from https://news.cgtn.com

Olingo, A. (2018). *Two Kenyan banks lose $0.86 million to hackers in a month*. Retrieved from https://www.theeastafrican.co.ke

Omar, M. B. & Kilika, J. (2018). Service delivery practices and performance of selected banks in Nairobi County, Kenya. *International Academic Journal of Human Resource and Business Administration, 3*(4), 228-249

Panda, A. & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment, 11*(4), 507-518.

Pandey, S., Gunasekaran, A. & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing, 13*(1), 103-128.

Parn, E.A. & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management, 26*(2), 245-266.

Rasphus, R. (2020). *Quality Service Delivery in Commercial Banks towards Customer Satisfaction: A Case of CRDB Bank –Mwanjelwa Branch*. Retrieved from http://scholar.mzumbe.ac.tz

Ross, R., Graubart, R. & Bodeau, D. (2018). *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. Retrieved from csrc.nist.gov.

Russell, R.B. (2013). *Social research method: qualitative and quantitative approaches*. Los Angeles: SAGE Publications.

Sallos, M.P., Garcia-Perez, A. & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital, 20*(4), 581-597.

Security Intelligence Solutions (2020). *Cyberrisk in banking: A review of the key industry threats and responses ahead.* Retrieved from http://www.ifconsultants.org

Siegal, L. & McCormick. (2016). *Criminology in Canada: Theories, Patterns, and Typologies* (3rd ed.). Toronto: Thompson, Nelson.

Stokes, P. & Wall, T. (2017). *Research Methods*. New York: Macmillan International.

Uddin, Md Hamid & Hakim, Bm & Hassan, M. Kabir. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management, 22*(10), 11-21.

Voss, T. (2013). The Rational Choice Approach to an Analysis of Intra- and Inter organizational Governance. *Research in the Sociology of Organizations, 20,* 21-46.

Weick, A., Rapp, C., Sullivan, W.P. & Kisthardt, W. (1989). A strengths perspective for social work practice. *Social Work, 34,* 350-354.

Wilson, J. (2014). *Essentials of business research: A guide to doing your research project*. Los Angeles, California: SAGE Publications.

Wilson, L.S. & Kwileck, S. (2013). Are These People Crazy, Or What? A Rational Choice Interpretation of Cults and Charisma. *Humanomics, 19*(1), 29-44.

Woodard, D. (2019). *Cyber Resilience through Deception and Decoy*. Retrieved from http://ceur-ws.org/Vol-2040/paper13.pdf

Yevale, N.A. (2016). *Research Methods the Basics.* Solapur: Laxmi Book Publications.

Zimmerman M. A. (2013). Resiliency theory: a strengths-based approach to research and practice for adolescent health. *Health education & behavior: the official publication of the Society for Public Health Education, 40*(4), 381–383.

APPENDICES

Appendix I: Questionnaire

<u>*Instructions*</u> *:*

Kindly, fill in all closed-ended questions by ticking the appropriate option. For the open-ended questions write the correct responses to the best of your knowledge. **Section A:General Information**

1. Gender

   Female [ ] Male [ ]

2. Age bracket

   18and30 yrs [ ] 31and40 yrs [ ]

   41-50yrs [ ] Above 50 yrs [ ]

3. Level of education

   Diploma/College Certificate [ ] Undergraduate [ ]

   Masters Degree [ ] PhD Degrees [ ]

   Other (Specify) ……………………………….

4. Duration of working?

   Less than 1 year [ ] 1 to 5 years [ ]

   6 to 10 years [ ] More than 10 years [ ]

Section B: Cyber Security Techniques

5. To what extent has the organization adopted the below cyber resilience techniques in the fight against cyber-attacks.

Cyber Resilience Techniques	**1**	**2**	**3**	**4**	**5**
Adaptive response					
Analytical monitoring					
Coordinated protection					
Deception					
Dynamic representation					
Dynamic positioning					

Privilege restriction					
Substantiated integrity					

6. To what extent do the cyber resilience techniques prevent the following cybercrimes against your bank?.

Cybercrimes	**1**	**2**	**3**	**4**	**5**
Email and phishing scams					
Identity theft					
Attacks on transaction channels					
Impersonation					
Fraud					
Forgery					
Unauthorized disclosure or passwords					
Fraudulent use of electronic data					
Online intrusion					
Malware					
Card information skimming					
Electronic money laundering					

7. Specify your agreement with the below statements on various cyber resilience techniques in your organization?.

Statement	**1**	**2**	**3**	**4**	**5**
Adaptive Response.					
Our organization uses agile and also alternative operational contingencies to ensure lowest operational capabilities even during attacks.					
Our organization limits consequences of cyber-attacks.					
Our organization takes preemptive action where appropriate.					
Analytic Monitoring.					
Our organization uses gathers and analyzes data to identify vulnerabilities.					
Our organization utilizes malware and forensic analysis to assess the actual damage by cyber-attacks.					
Coordinated Protection.					
Our organization uses multiple and distinct mechanisms to					

protect systems and sub-systems ,					
Use of coordinated protection makes it hard for adversary to attack successfully.					
Use of coordinated protection raises the likelihood of adversary detection.					
Deception.					
Our organization uses deception technology to confuse and mislead adversaries.					
Deception technology is used to delay the effect of attack.					
Deception technology causes the adversary to misdirect or waste its resources.					
Dynamic Representation.					
Our organization uses dynamic mapping and profiling.					
Our organization makes use of dynamic threat modeling.					
Our organization keeps on changing systems					
Dynamic Positioning.					
Our organization frequently relocates functionality.					
Our organization ensures asset mobility to change attack surface.					
Privilege Restriction.					
Our organization restricts the use of systems and sub-systems.					
Our organization limits the probability that unintended actions by authorized individuals					
Use of cyber resilience curtails the adversary’s ability to take credentials’ full advantage.					
Substantiated Integrity.					
Our organization provides mechanisms to ascertain whether critical services have been corrupted.					
Our organization provides mechanisms to evaluate if information stores have been corrupted.					
Our organization provides mechanisms to evaluate if information streams have been corrupted.					

Cyber Resilience

8. Specify the degree to which your organization achieves the below cyber resilience goals during cyber-crime?

Statement	**1**	**2**	**3**	**4**	**5**
Anticipate					
Withstand					
Recover					
Evolve					

9. How frequent does your organization experience service disruptions?

Every week [ ]

Every month [ ]

Every six months [ ]

10. How long does it take to recover from incidences? ………………….

11. How many incidences are prevented in a month in your organization? ………………….

12. How can cyber resiliency in Kenyan commercial banks be improved?

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………